Two Essays on the Impact of Cybersecurity Risk Management Examinations on Investor Perceptions and Decisions

Rebecca R. Perols

*University of South Florida, rperols@hotmail.com*
Two Essays on the Impact of Cybersecurity Risk Management Examinations on Investor Perceptions and Decisions

by

Rebecca R. Perols

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Business Administration with a concentration in Accounting
Lynn Pippenger School of Accountancy
Muma College of Business
University of South Florida

Major Professor: Uday Murthy, Ph.D.  
Lisa Gaynor, Ph.D.  
Patrick Wheeler, Ph.D.  
Terry Sincich, Ph.D.

Date of Approval:  
March 7, 2019

Keywords: Non-Audit Services, Audit Quality, Independence, Assurance, Voluntary Disclosure, Cybersecurity Incidents

Copyright © 2019, Rebecca R. Perols
Dedication

To Johan, thank you for your amazing support and encouragement at every step of this process, and to Noah and Lukas, who were so young when we started this adventure, thank you for bringing a wonderful perspective and the motivation to persevere and succeed.
Acknowledgments

I would like to first thank my dissertation committee, Dr. Murthy, Dr. Gaynor, Dr. Wheeler, and Dr. Sincich, for their tremendous support throughout the dissertation process and the Ph.D. program. I am especially thankful to Dr. Murthy for initially encouraging me to pursue a Ph.D. and for consistently providing me timely, constructive, and insightful feedback on my work throughout the entire Ph.D. program – no matter how busy he was. I am truly grateful.

I also thank Jane Jollineau, Dahlia Robinson, Tom Smith, Mark Mellon, Peter Kipp, Joyce Cheng, James Zhang, Ian Zhang, Stephanie Walton, Becca Baske, and Hilda Carrillo for providing helpful feedback on my work and for supporting me during the Ph.D. program.

Finally, I thank my family and friends for encouraging me to complete my dissertation and for helping me celebrate my incremental achievements throughout the Ph.D. program.
Table of Contents

List of Tables ........................................................................................................................................ iii

List of Figures ......................................................................................................................................... iv

Abstract .................................................................................................................................................. v

Chapter 1. Dissertation Overview ........................................................................................................... 1
  1.1 Overall Motivation .......................................................................................................................... 1
  1.2 Overview of the Two Essays .......................................................................................................... 2
  1.3 Figure of Dissertation Overview .................................................................................................. 3

Chapter 2. Essay 1: The Impact of Cybersecurity Risk Management Examinations and
Cybersecurity Incidents on Investor Perceptions and Decisions .................................................... 4
  2.1 Introduction .................................................................................................................................... 4
  2.2 Theory and Hypotheses Development ............................................................................................. 10
    2.2.1 Background and Theoretical Foundation .............................................................................. 10
    2.2.2 The Effect of Jointly Provisioned Cybersecurity Examinations ......................................... 12
    2.2.3 The Impact of Subsequent Cybersecurity Incidents ............................................................... 15
    2.2.4 Perceptions of Competence, Independence, and Audit Quality .............................................. 17
  2.3 Research Method ............................................................................................................................. 20
    2.3.1 Participants .............................................................................................................................. 20
    2.3.2 Experimental Task and Design ............................................................................................... 20
    2.3.3 Dependent Variable .................................................................................................................. 22
    2.3.4 Other Measured Variables ....................................................................................................... 23
    2.3.5 Pilot Study ............................................................................................................................... 24
  2.4 Results ............................................................................................................................................. 26
    2.4.1 Descriptive Statistics ................................................................................................................ 26
    2.4.2 Tests of Hypotheses ................................................................................................................ 27
    2.4.3 Summary of Results ................................................................................................................ 29
  2.5 Conclusion ........................................................................................................................................ 30
  2.6 Tables for Essay 1 ............................................................................................................................ 35
  2.7 Figures for Essay 1 ........................................................................................................................... 39

Chapter 3. Essay 2: The Impact of the Type of Cybersecurity Assurance Service and
Cybersecurity Incidents on Investor Perceptions and Decisions .................................................... 41
  3.1 Introduction ....................................................................................................................................... 41
  3.2 Theory and Hypotheses Development ............................................................................................. 47
    3.2.1 External Assurance .................................................................................................................. 47
    3.2.2 Cybersecurity Incidents .......................................................................................................... 50
    3.2.3 Perceptions of Cybersecurity Assurance Services Quality .................................................. 52
List of Tables

Table 2.1: Essay 1 Descriptive Statistics – Mean (Standard Deviation) .......................................................35
Table 2.2: The Effect of Provisioning Type and Cybersecurity Incident on Willingness to Invest ..................................................36
Table 2.3: Results of Hypothesized Model ..........................................................................................37
Table 2.4: Summary of Hypotheses Testing ..................................................................................38
Table 3.1: Essay 2 Descriptive Statistics – Mean (Standard Deviation) .............................................69
Table 3.2: The Effect of Type of Cybersecurity Assurance Service and Cybersecurity Incident on Willingness to Invest ..................................................................................70
Table 3.3: Indirect Effects of Type of Cybersecurity Assurance Service on Willingness to Invest ..................................................................................71
Table 3.4: Conditional Indirect Effects of Type of Assurance on Willingness to Invest ............72
List of Figures

Figure 1.1: Dissertation Overview ............................................................................................... 3

Figure 2.1: Hypothesized Model .................................................................................................39

Figure 2.2: Hypotheses Results with Path Coefficients (p-values) .............................................40

Figure 3.1: Perceptions of Cybersecurity Assurance Services Quality Mediation Analysis ......73

Figure 3.2: Perceptions of Management Credibility Mediation Analysis ..................................74

Figure 3.1: Perceptions of Cybersecurity Assurance Services Quality: Prevent versus
Recover Mediation Analysis ......................................................................................................75
Abstract

The goal of this dissertation is to investigate the impact of the American Institute of Certified Public Accountants’ (AICPA) recently adopted cybersecurity risk management examination on investor perceptions and decisions. The dissertation implements a two-essay approach.

Essay 1 examines the effect of voluntary disclosures of joint or separate provisioning of cybersecurity risk management examinations on investor perceptions and decisions, and whether these effects differ when a subsequent cybersecurity incident occurs. Conducting a 2 x 2 between-participants experiment, I find that the negative signal of a subsequent cybersecurity incident reverses investors’ positive perceptions of auditor competence and increases investors’ sensitivity to potential independence impairments when the cybersecurity risk management examination is jointly provisioned, leading to lower perceptions of audit quality. I also find that investors are less willing to invest when the cybersecurity risk management examination is jointly compared to separately provisioned. My results provide important insights to regulators and standard setters who have raised concerns regarding the importance of addressing cybersecurity risk in the integrated internal control over financial reporting and financial statements audits and the potential for independence impairments from increased auditor performed non-audit services such as cybersecurity. My study also contributes to the non-audit services literature not only by examining a unique and emerging non-audit service not previously examined, but also by showing that non-audit services are perceived differently depending on whether a negative signal of non-audit service quality is present.
Essay 2 examines the effect of the type of cybersecurity assurance service on investor perceptions and decisions and whether these effects differ when a prior cybersecurity incident is reported. Conducting a 2 x 2 between-participants experiment, I find that investors are more willing to invest and have higher perceptions of management credibility when voluntary disclosures include a cybersecurity risk management examination compared to a less comprehensive cybersecurity assurance service. These findings are important because public company boards are increasingly looking to audit firms to provide cybersecurity assurance services. I also find that investors perceive cybersecurity risk management examinations to provide higher assurance quality regarding an organization’s ability not only to prevent future cybersecurity incidents, but also to recover from future cybersecurity incidents that are not prevented - a key risk management issue raised by regulators. My study also contributes to the voluntary assurance disclosure literature by examining investor reactions to management disclosures of alternative types of voluntary external cybersecurity assurance services, beyond a comparison of the absence or presence of external assurance reports provided by CPAs previously examined in other non-financial voluntary assurance settings. I also find that management’s choice to acquire a more comprehensive cybersecurity assurance service has a positive effect on investors’ perceptions of management credibility, which in turn has a positive effect on investors’ willingness to invest.

This dissertation contributes to the growing literature related to cybersecurity. Most of this work has been archival in nature and as such, has not been able to examine the effects of the AICPA’s recently adopted cybersecurity risk management examination reporting. Using an experimental method, I am able to examine important implications of voluntary cybersecurity risk management examination reporting and present opportunities for future research.
Chapter 1. Dissertation Overview

1.1 Overall Motivation

With the goal of providing more complete and useful information to investors, the Securities and Exchange Committee (SEC) recently issued guidance for public company cybersecurity risk and incident disclosures including information about cybersecurity risk management programs and preventative actions taken to reduce cybersecurity risks (SEC 2018a). In response to increased cybersecurity risk and the growing demand for information about how organizations are managing cybersecurity risk, the American Institute of Certified Public Accountants (AICPA) recently released a new cybersecurity risk management examination service designed to provide external assurance related to the effectiveness of an organization’s cybersecurity risk management program (AICPA 2017a). A cybersecurity risk management program is “a set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity’s cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented” (AICPA 2017b, 207).

The AICPA’s new cybersecurity risk management examination service provides a general-use report intended to benefit a broad range of potential users including investors (AICPA 2017a); however, it is unclear how nonprofessional investor perceptions and decisions will be impacted by organizations’ voluntary cybersecurity risk management examination disclosures. In addition, cybersecurity incidents are often highly publicized in the news, are increasing, and are required to be disclosed if material (SEC 2011, 2017a). It is possible that an
organization’s disclosure of a significant cybersecurity incident could impact investor reactions to that organization’s voluntary cybersecurity risk management examination disclosure. As such, the overall goal of this dissertation is to investigate the impact of voluntary cybersecurity risk management examination disclosures on investor perceptions and decisions.

1.2 Overview of the Two Essays

Figure 1.1 provides an overview of the dissertation and the relationships among the two essays. Essay 1 and Essay 2 read as standalone essays and can be read in any order. The dissertation examines the effects of three independent constructs: provisioning type, cybersecurity incident, and type of cybersecurity assurance service. In Essay 1, provisioning type is operationalized as joint provisioning or separate provisioning because cybersecurity risk management examinations are classified as permitted non-audit services and organizations can obtain cybersecurity risk management examination services from their existing financial statement auditors, i.e., joint provisioning, or from a separate provider (U.S. Congress 2002; SEC 2003). Cybersecurity incident is operationalized in Essay 1 as the absence or presence of a cybersecurity incident subsequent to a voluntary cybersecurity risk management examination disclosure and in Essay 2 as the absence or presence of a cybersecurity incident prior to a voluntary cybersecurity risk management examination disclosure. In Essay 2, type of cybersecurity assurance service is operationalized as a more or less comprehensive assurance service because cybersecurity assurance services can differ in terms of the comprehensiveness of the subject matter (AICPA 2017b).

Essay 1 draws on source credibility theory (Birnbaum and Stegner 1979) and DeAngelo’s (1981) theoretical audit quality model to develop hypotheses regarding the impact of provisioning type and cybersecurity incident on investor perceptions and decisions. Essay 2
draws on dual processing theories (Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003) and Mercer’s (2004) management disclosure framework to develop hypotheses regarding the impact of type of cybersecurity assurance service and cybersecurity incident on investor perceptions and decisions.

The remainder of the dissertation is organized as follows. Chapter 2 presents Essay 1 as a standalone essay and Chapter 3 presents Essay 2 as a standalone essay. Chapter 4 concludes the dissertation.

1.3 Figure of Dissertation Overview

![Diagram of Dissertation Overview]

Figure 1.1: Dissertation Overview

2.1 Introduction

Cybersecurity risk is increasingly viewed as one of the most significant challenges facing companies in the U.S. (KPMG 2018; PwC 2019). Cybercrime can result in reputational damage, loss of intellectual property, disruption of business operations, government fines, and litigation expenses (AICPA 2017a; CAQ 2016a). In response to these risks and the growing demand for information about organizations’ cybersecurity risk management programs,1 the American Institute of Certified Public Accountants (AICPA) has released a new examination-level attestation service designed to provide assurance related to the effectiveness of organizations’ cybersecurity controls (AICPA 2017a). The cybersecurity risk management examination is a voluntary, general-use report that is intended to benefit a broad range of potential users including investors, directors, analysts, and regulators (AICPA 2017a; CAQ 2016a).2

Recent high-profile cybersecurity breaches at public companies (e.g., Target, Home Depot, Sony) have heightened the general public’s and investors’ sensitivity to such incidents. As public companies increasingly seek to provide voluntary cybersecurity risk management

---

1 A cybersecurity risk management program is a “…set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity’s cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented” (AICPA 2017b, 207).

2 System and Organization Controls (SOC) for Cybersecurity examinations include three components: (1) management’s description of the cybersecurity risk management program, (2) management’s assertion that the description is presented in accordance with the AICPA’s description criteria and the controls within the program were effective based on the control criteria, AICPA’s Trust Services or alternatives, and (3) the CPA’s opinion on management’s description and the effectiveness of the controls within the program (AICPA 2017a).
examination disclosures, it is unclear how nonprofessional (retail) investors will perceive such disclosures. Accordingly, the AICPA has called for research that explores how users respond to cybersecurity risk management examination reporting (AAA 2017a, 2017b). Moreover, the Securities and Exchange Commission (SEC) is particularly concerned about cybersecurity threats facing nonprofessional (retail) investors and the need for more robust cybersecurity disclosures, including more information about organizations’ cybersecurity risk management programs and preventative actions taken to reduce and manage cybersecurity risk (SEC 2017b, 2018a).

Cybersecurity risk management examinations are classified as permitted non-audit services and organizations can obtain cybersecurity risk management examination services from their financial statement auditors, i.e., joint provisioning, or from a separate provider (U.S. Congress 2002; SEC 2003). Joint provisioning of cybersecurity risk management examinations could potentially have both functional and dysfunctional effects on the work performed by the audit firm. The work performed in cybersecurity risk management examinations overlaps with the assurance work performed in integrated internal control over financial reporting (ICFR) and financial statements audits and the Public Company Accounting Oversight Board (PCAOB) has emphasized the importance of auditors increasingly considering cybersecurity risks in the integrated audits (PCAOB 2016, 2018). This overlap between cybersecurity risk management

---

3 With the goal of improving auditor independence and financial reporting quality, the Sarbanes-Oxley Act of 2002 (SOX) and related Securities and Exchange Commission (SEC) rules: (1) banned audit firms from providing certain non-audit services such as financial information system design and implementation and internal audit services to audit clients; (2) increased disclosure requirements related to audit and non-audit services fees; and (3) required audit committees to pre-approve both audit and permitted non-audit services (U.S. Congress 2002; SEC 2003). There is no prohibition in SOX against the independent auditor also providing cybersecurity examination services.

4 Not only is an understanding of the client’s business processes and information systems important in both cybersecurity examinations and ICFR audits, many entity-level controls, e.g., control environment, risk assessment procedures, monitoring, general computer controls, etc., are also important to understand and test in both cybersecurity examinations and ICFR audits. PCAOB staff inspection briefs continue to highlight concerns about
examinations and the integrated audits and increased importance of cybersecurity risk in the integrated audits creates an opportunity for increased auditor competence from knowledge spillover effects and from making it more cost-effective to use specialists who are more competent. The potential synergy between cybersecurity risk management examinations and the integrated audits is thus a functional effect of joint provisioning.

On the other hand, the Investor Advisory Group of the PCAOB has raised concerns that the rise of non-audit services, including cybersecurity services, in the large public auditing firms is threatening auditor independence and increasing risks to nonprofessional investors (PCAOB 2014). Joint provisioning of cybersecurity risk management examinations could result in a dysfunctional effect if investors perceive an impairment in auditor independence from providing the non-audit service. Given the overlap between cybersecurity risk management examinations and the integrated ICFR and financial statements audits that may result in increased auditor competence and the concern about auditor independence impairments, the cybersecurity context provides an interesting setting to examine investor perceptions of the functional and dysfunctional effects of joint provisioning. In this study, I investigate the effect of joint compared to separate provisioning of cybersecurity risk management examinations on investor perceptions and decisions.

The cybersecurity risk management examination context is also of interest given the potential for a subsequent cybersecurity incident and ensuing investor reactions. The occurrence of a significant cybersecurity incident following a jointly provisioned cybersecurity auditors’ procedures for assessing risks related to cybersecurity that could have an effect on the financial statements audit and how these risks are addressed, i.e., how engagement teams modify their audit approach based on these risks, including how changes are made to audit procedures to test ICFR (PCAOB 2016, 2018).

5 Cybersecurity incidents are often highly publicized in the news, are increasing, and are required to be disclosed if material (SEC 2011, 2017a). The consequences of cybersecurity incidents to investors can be significant as illustrated by Equifax’s stock falling 31% and losing over $5 billion in market value when the magnitude of Equifax’s 2017 cybersecurity breach was disclosed (Reklaitis 2017; SEC 2018b).
risk management examination could be perceived by investors as a negative signal not only of the quality of the cybersecurity risk management examination but also of the integrated ICFR and financial statements audits. In the event of a subsequent cybersecurity incident, investor perceptions of the positive effects of increased competence from joint provisioning could be outweighed by perceptions of the negative effects of independence impairment from joint provisioning. I examine if the effect of a subsequent cybersecurity incident on investor perceptions and decisions differs depending on whether the cybersecurity risk management examination is provisioned jointly or separately.

Drawing on source credibility theory (Birnbaum and Stegner 1979), DeAngelo’s (1981) theoretical audit quality model, and Wallace’s (1987) information hypothesis I develop predictions for how and why joint provisioning and subsequent cybersecurity incidents impact investor perceptions and decisions. I conduct an experiment using a 2 x 2 between-participant design and manipulate (1) cybersecurity examination provisioning type as joint or separate and (2) subsequent cybersecurity incident as a cybersecurity incident absent or present following the cybersecurity risk management examination disclosure. I measure how my manipulations impact investors’ willingness to invest (e.g., Koonce and Lipe 2010; Elliott, Rennekamp, and White 2015; Asay, Libby, and Rennekamp 2018). To understand why my manipulations impact willingness to invest, I measure perceptions of auditor independence (Beattie, Brandt, and Fearnley 1999; Lowe, Geiger, and Pany 1999; SEC 2001), auditor competence (Bassellier, Benbasat, and Reich 2003; AICPA 2016), and audit quality (Gaynor, Kelton, Mercer, and Yohn 2016; PCAOB 2007).

Consistent with my predictions that joint provisioning of the cybersecurity risk management examination creates an opportunity for increased auditor competence from
knowledge spillover effects, my results indicate that in the absence of a cybersecurity incident, investors’ perceptions of auditor competence are greater when the cybersecurity risk management examination is provisioned jointly compared to separately. I also find that when the cybersecurity risk management examination is provisioned jointly, the negative signal of a subsequent cybersecurity incident reverses investors’ positive perceptions of competence and increases investors’ sensitivity to potential independence impairments. Overall, my results indicate that investors are more willing to invest in a company when the cybersecurity risk management examination is provisioned separately compared to jointly – a finding that has important implications for public companies and their boards.

This study makes three contributions. First, I contribute to the growing literature related to cybersecurity. Most of this work has been archival in nature and as such, has not been able to examine the effects of the AICPA’s new cybersecurity risk management examination reporting. Using an experimental method, I am able to examine a potentially important implication of how cybersecurity risk management examinations are provisioned. Specifically, I find that investors are less willing to invest when the cybersecurity risk management examination is jointly compared to separately provisioned.

Second, this paper contributes to the research stream on non-audit services by not only examining investor perceptions of joint provisioning of cybersecurity risk management examinations, a unique and emerging non-audit service not previously examined, but also by providing insights into the longstanding debate over the theorized competing (i.e., suppressing) effects of increased competence and decreased independence on audit quality. Schneider, Church, and Ely (2006) highlight that future research should focus on specific types of non-audit services rather than the broad and varying non-audit services fee categories used in many prior
studies providing mixed results. Interestingly, I find that the negative signal of a subsequent cybersecurity incident reverses investors’ positive perceptions of competence and increases investors’ sensitivity to potential independence impairments. Further, both competence and independence perceptions have positive effects on perceptions of audit quality. These results show that non-audit services are perceived differently depending on whether a negative signal of non-audit service quality is present and highlight the importance of measuring perceptions of both independence and competence when evaluating how non-audit services affect perceptions of audit quality.

Third, this study contributes to purchasers of cybersecurity risk management examinations and informs regulators and standard setters by examining investors’ reactions to the AICPA’s recently adopted voluntary cybersecurity risk management examination reporting. My results indicate that it might be advantageous for purchasers of cybersecurity risk management examinations to provision the cybersecurity risk management examination separately from the audit due to the negative effect of joint provisioning on investors’ willingness to invest – an important finding given that cybersecurity has become a top concern for public companies and their boards (NACD 2017) who are looking to their auditors to provide cybersecurity services both within and outside the scope of the integrated ICFR and financial statements audits (AAA 2019). My findings also provide insights to regulators and standard setters considering changes to the voluntary nature of provisioning guidelines of cybersecurity risk management examinations. The PCAOB has emphasized the importance of auditors increasingly considering components of cybersecurity in the integrated ICFR and financial statements audits (PCAOB 2016, 2018), while also raising concerns that the rise of non-audit services, including cybersecurity services, is threatening auditor independence in the large public
auditing firms and increasing risks to nonprofessional investors (PCAOB 2014). Despite investors’ perceptions of increased competence consistent with the opportunity for knowledge spillover, in the event of a cybersecurity incident investors’ perceptions of audit quality is reduced when the cybersecurity risk management examination is provisioned jointly.

2.2 Theory and Hypotheses Development

2.2.1 Background and Theoretical Foundation

In order to understand how and why the joint provisioning of cybersecurity risk management examinations impacts investor perceptions and decisions I first discuss the debate in the literature regarding the positive (functional) and potentially negative (dysfunctional) effects of joint provisioning. I then present the expected theoretical relations that together explain the overall effect of joint provisioning on investors’ willingness to invest.

On one hand, non-audit services are typically conjectured to impair auditor independence in fact or appearance, presumably because the additional revenue increases the importance of the client to the auditor, i.e., economic dependence, making it more likely that the auditor will agree to management’s preferred positions, which in turn decreases audit quality (e.g., Frankel, Johnson, and Nelson 2002; Kinney, Palmrose, and Scholz 2004; Krishnan, Hebatollah, and Zhang 2005; Francis 2006; Francis and Ke 2006; Gaynor, McDaniel, and Neal, 2006; Khurana and Raman 2006; Srinidhi and Gul, 2007). On the other hand, non-audit services are also conjectured to increase auditor competency and efficiency, presumably through knowledge spillover effects and increased use of specialists, which in turn increases audit quality (e.g., Simunic 1984; Whisenant, Sankaraguruswamy, and Raghunandan 2003; Kinney et al. 2004;

In support of the effects of independence and competence on audit quality, the theoretical model developed by DeAngelo (1981) explains that the quality of external assurance is impacted by two factors, the independence and competence of the assurance provider. External assurance providers who are more independent and more competent provide higher quality external assurance. Similarly, source credibility theory posits that individuals evaluate the credibility of an information source based on the potential bias from the source and the expertise of the source (Birnbaum and Stegner 1979). Individuals’ use of credibility as a cognitive heuristic when evaluating new information has been supported in psychology research (e.g., Hovland, Janis, and Kelley 1953; Eagly, Wood, and Chaiken 1978; Chaiken and Maheswaran 1994) and in accounting research (e.g., Hirst, Koonce, and Simko 1995; Hirst, Koonce, and Miller 1999; Mercer 2004; Mercer 2005; DeZoort, Houston, and Hermanson 2003; Hodge, Hopkins, and Pratt 2006; Kim, Green, and Johnstone 2016). Together, the theoretical model developed by DeAngelo (1981) and source credibility theory (Birnbaum and Stegner 1979) suggest that individuals’ perceptions of assurance provider independence and competence are positively related to perceptions of external assurance quality.

Consistent with Wallace’s (1987) information hypothesis stating that independent assurance reduces information asymmetry and uncertainty, external assurance quality has a positive impact on investor perceptions of the credibility of the subject matter and the extent to which investors rely on the subject matter in making valuation judgments (e.g., Libby 1979; Hodge 2001, Coram, Monroe, and Woodliff (2009). In other words, assurance quality is
positively related to the extent to which investors react more positively to positive news and
more negatively to negative news in their valuation judgments (Coram et al. 2009).

2.2.2 The Effect of Jointly Provisioned Cybersecurity Examinations

Following this theoretical foundation and background about the effects of joint
provisioning of non-audit services, I expect that joint provisioning of cybersecurity risk
management examinations will have a positive effect on perceptions of auditor competence, a
negative effect on perceptions of auditor independence, and that perceptions of competence and
independence will in turn have positive effects on perceptions on audit quality, which is
positively related to valuation judgments (i.e., willingness to invest). While these individual
effects are supported directly by the theoretical foundation, it is less clear what the overall effect
of joint provisioning will be on willingness to invest due to the competing positive effect of
competence and negative effect of independence. To make an overall prediction about the effect
of joint provisioning on willingness to invest I next turn to prior literature.

Prior research examining whether the provision of other non-audit services is associated
with lower financial reporting and audit quality has yielded mixed results. On one hand, non-
audit services are associated with lower financial reporting quality, including accruals (Frankel et
al. 2002; Srinidhi and Gul, 2007) and restatements (Kinney et al. 2004), negative stock price
reactions (Krishnan et al. 2005; Francis and Ke 2006) and higher cost of equity (Khurana and
Raman 2006). These results are consistent with auditor independence impairments due to joint
provisioning having a stronger negative effect than the potential positive effect from increased
competence. On the other hand, research has found evidence of positive overall net effects
associated with joint provisioning such as increased financial reporting and audit quality
(Robinson 2008; Gleason and Mills 2011), reduced audit reporting lags (Knechel and Sharma 2011), lower accounting risk (Prawitt et al. 2012), and improved earnings quality (Koh et al. 2013). These findings suggest that in some settings, the positive effect from increased competence due to joint provisioning is stronger than the negative effect associated with auditor independence impairments.

Schneider et al. (2006) suggests that the broad and varying non-audit services fee categories used in many prior studies have contributed to the mixed results and that the specific type of non-audit service and context is important. In the cybersecurity context, there is a relatively substantial overlap between cybersecurity risk management examination procedures and integrated audit procedures. In both cybersecurity risk management examinations and integrated audits, an understanding of the client’s business processes and information systems is important. Similarly, many entity-level controls, e.g., control environment, risk assessment procedures, monitoring, general computer controls, etc., are important to understand and test in both cybersecurity risk management examinations and integrated audits. Additionally, the PCAOB staff inspection briefs continue to highlight concerns about auditors’ procedures for assessing risks related to cybersecurity that could have an effect on the financial statements audit and how these risks are addressed, i.e., how engagement teams modify their audit approach based on these risks, including how changes are made to audit procedures to test ICFR (PCAOB 2016; 2018). Similarly, the Center for Audit Quality (CAQ) has also emphasized the importance of auditors considering components of cybersecurity in the integrated audits (CAQ 2016b).6

---

6 The CAQ issued guidance explaining that “auditing standards require the auditor to obtain an understanding of how the company uses IT and the impact of IT on the financial statements, the extent of the company’s automated controls as they relate to financial reporting, including the IT general controls that are important to the effective operation of automated controls, and the reliability of data and reports used in the audit that were produced by the company. In assessing the risks of material misstatement to the financial statements—including IT risks resulting from unauthorized access—auditors are required to take into account their understanding of the company’s IT
The overlap between cybersecurity risk management examinations and integrated audits and the increased importance of cybersecurity risk in the integrated audits provide a strong opportunity for knowledge spillover. This overlap could result in greater synergy if a single firm performs both services, which could make it more cost-effective to use specialists who are more competent. This overlap also increases the likelihood that the same group or individuals perform both services, resulting in greater knowledge spillover effects. Consequently, the positive effects of having cybersecurity risk management examinations and integrated audits performed by the same firm could be stronger than the positive effects of joint provisioning of some other non-audit services.

To make a prediction as to whether perceptions of the positive effect associated with competence improvements will outweigh perceptions of the negative effect associated with independence impairments, I rely on Prawitt et al. (2012) who examine a setting where the overlap between the non-audit service and the audit is substantial. Prawitt et al. (2012) show that pre-SOX Big N internal audit outsourcing (i.e., joint provisioning of internal audit non-audit services) is associated with lower accounting risk. I note that Prawitt et al. (2012) employ a proxy for actual financial reporting and audit quality, whereas I measure investor perceptions, and the overlap in an internal audit outsourcing setting might arguably be even greater than in the cybersecurity risk management examination setting. Still, their findings suggest that the positive effect from improvements in competence due to joint provisioning may be stronger than the negative effect from auditor independence impairments.

Based on the strong opportunity for knowledge spillover, the increased importance of cybersecurity risk in the integrated audits (PCAOB 2016, 2018; CAQ 2016b), and the findings in systems and controls. If information about a material breach is identified, the auditor would need to consider the impact on financial reporting, including disclosures, and the impact on ICFR” (CAQ 2016b, 1).
Prawitt et al. (2012), I expect that when cybersecurity risk management examinations are jointly 
provisioned the theorized positive effect on competence will outweigh the theorized negative 
effect on independence. Drawing again on DeAngelo’s (1981) theoretical audit quality model 
and source credibility theory (Birnbaum and Stegner 1979), I expect that, absent a cybersecurity 
incident, investors will perceive joint provisioning, due to the expected stronger effect on 
competence relative to independence, to result in perceptions of higher quality external 
assurance. Drawing again on Wallace’s (1987) information hypothesis and prior literature (e.g., 
Libby 1979; Hodge 2001, Coram et al. 2009), perceptions of higher quality external assurance 
will lead to higher valuations judgments (e.g., willingness to invest). My first hypothesis 
follows:

**H1:** In the absence of a cybersecurity incident, investors will be more willing to invest 
when the cybersecurity examination is jointly compared to separately provisioned.

### 2.2.3 The Impact of Subsequent Cybersecurity Incidents

Cybersecurity incidents are often highly publicized in the news, are increasing, and are 
required to be disclosed if material (SEC 2011, 2017a). Cybersecurity incidents can be costly in 
terms of remediation effort, system downtime, and damaged reputation and trust, which is likely 
why prior research has demonstrated a negative market reaction to reported cybersecurity 
incidents (e.g., Campbell, Gordon, Loeb, and Zhou 2003; Goel and Shawky, 2009; Gatzlaff and 
McCullough, 2010; Hinz, Nofer, Schiereck, and Trillig 2015). Consistent with these archival 
findings, I expect a negative effect of a cybersecurity incident on willingness to invest.

Additionally, a subsequent cybersecurity incident occurring after the issuance of the 
cybersecurity risk management examination report can provide a negative external signal to 
investors about external assurance quality. If provisioned separately, a subsequent cybersecurity
incident should primarily provide a negative signal of cybersecurity risk management examination quality given that the cybersecurity risk management examination is not performed by the audit firm. However, when the cybersecurity risk management examination is jointly provisioned, the signal could also reduce investors’ perceptions of the quality of the integrated audit work. More specifically, I expect that a subsequent cybersecurity incident will send a negative signal of external assurance quality, increasing investors’ sensitivity to potential independence impairments and reducing investors’ perceptions of auditor competence, with these effects being revealed through a lower willingness to invest.

Drawing again on DeAngelo’s (1981) theoretical audit quality model and source credibility theory (Birnbaum and Stegner 1979), in the event of a subsequent cybersecurity incident I expect that the negative signal of a subsequent cybersecurity incident will have a greater negative effect on investors’ perceptions of auditor competence and independence, resulting in a greater negative effect on perceptions of external assurance quality, when the cybersecurity risk management examination is provisioned jointly compared to separately. Drawing again on Wallace’s (1987) information hypothesis and prior literature (e.g., Libby 1979; Hodge 2001, Coram et al. 2009), perceptions of external assurance quality will impact valuations judgments (e.g., willingness to invest). Based on this discussion, I present the following hypotheses:

**H2a**: A subsequent cybersecurity incident will negatively impact willingness to invest.

**H2b**: A subsequent cybersecurity incident will have a negative effect on the relation between provisioning type and willingness to invest.


2.2.4 Perceptions of Competence, Independence, and Audit Quality

Figure 2.1 presents my model of how jointly provisioned cybersecurity risk management examinations in the presence or absence of a cybersecurity incident affect investors’ willingness to invest through the perceptual variables of auditor competence, auditor independence, and audit quality. I next explain my hypotheses in relation to this model.

Perceptions of Competence and Independence. The theoretical model developed by DeAngelo (1981) explains that the quality of external assurance is impacted by primarily two factors, the competence and independence of the assurance provider. Similarly, source credibility theory posits that individuals evaluate the credibility of an information source based on the potential bias from the source and the expertise of the source (Birnbaum and Stegner 1979). Consistent with DeAngelo (1981) and source credibility theory (Birnbaum and Stegner 1979), the longstanding debate over non-audit services has also focused primarily on two competing factors: competence and independence. On one side of the debate, non-audit services increase auditor competence through knowledge spillover effects, while on the other side of the debate non-audit services impair auditor independence through economic dependence (e.g., Schneider et al. 2006). Similar to some prior research on other non-audit services finding positive effects of joint provisioning (e.g., Prawitt et al. 2012), the cybersecurity risk management examination setting provides a strong opportunity for knowledge spillover due to the overlap between the cybersecurity risk management examination and the integrated ICFR and financial statements audits. As discussed earlier and as conjectured earlier by research examining the net effect of non-audit services, I expect that investors will perceive joint provisioning to increase auditor competence (Robinson 2008; Lai and Krishnan 2009; Gleason and Mills 2011; Knechel and Sharma 2011; Prawitt et al. 2012; Koh et al. 2013) and that
investors will perceive joint provisioning to impair independence due to increased economic
dependence on the client (Krishnan et al. 2005; Francis 2006; Francis and Ke 2006; Gaynor et al.
2006; Khurana and Raman 2006; DeFond and Zhang 2014). Accordingly, I present the
following hypotheses:

**H3a**: In the absence of a cybersecurity incident, perceptions of competence will be
greater when the cybersecurity examination is jointly compared to separately
provisioned.

**H3b**: In the absence of a cybersecurity incident, perceptions of independence will be
lower when the cybersecurity examination is jointly compared to separately
provisioned.

*The Effect of a Subsequent Cybersecurity Incident*. When the cybersecurity risk
management examination is jointly provisioned, I expect that a subsequent cybersecurity incident
will send a negative signal of not only the cybersecurity risk management examination, but also
of the integrated ICFR and financial statements audits. Drawing again on DeAngelo’s (1981)
theoretical audit quality model and source credibility theory (Birnbaum and Stegner 1979) I
expect that investors will associate this negative signal with lower auditor competence and
independence when the cybersecurity risk management examination is jointly provisioned. That
is, investors will no longer perceive a positive effect of knowledge spillover from joint
provisioning and will also be more sensitive to independence impairment concerns from joint
provisioning. Therefore, I propose the following hypotheses:

**H4a**: A cybersecurity incident will have a negative effect on the relation between
provisioning type and investors’ perceptions of auditor competence.

**H4b**: A cybersecurity incident will have a negative effect on the relation between
provisioning type and investors’ perceptions of auditor independence.
**Perceptions of Audit Quality.** The theoretical model developed by DeAngelo (1981) posits that the quality of external assurance is impacted by two factors, the independence and competence of the assurance provider. Similarly, source credibility theory posits that individuals evaluate the credibility of an information source based on the potential bias from the source and the expertise of the source (Birnbaum and Stegner 1979). Together, the theoretical model developed by DeAngelo (1981) and source credibility theory (Birnbaum and Stegner 1979) suggest that individuals’ perceptions of assurance provider independence and competence are positively related to perceptions of external assurance quality. Although prior studies have not directly measured individual investors’ perceptions of both independence and competence and their effect on perceptions of audit quality, some support for these associations has been found in prior research (e.g., Swanger and Chewning 2001; Schneider et al. 2006; Prawitt, Smith, and Wood 2009; DeFond and Zhang 2014; Abbott, Daugherty, Parker, and Peters 2016).

Accordingly, I present the following hypotheses:

**H5a:** Perceptions of competence are positively associated with perceptions of audit quality.

**H5b:** Perceptions of independence are positively associated with perceptions of audit quality.

Consistent with Wallace’s (1987) information hypothesis stating that independent assurance reduces information asymmetry and uncertainty, external assurance quality has a positive impact on investor perceptions of the credibility of the subject matter and the extent to which investors rely on the subject matter in making valuation judgments (e.g., Libby 1979; Hodge 2001, Coram et al. 2009). In other words, assurance quality is positively related to the extent to which investors react more positively to positive news and more negatively to negative news in their valuation judgments (Coram et al. 2009). Given the positive news in my study, I
expect that perceptions of higher quality external assurance will lead to higher valuation judgments (e.g., willingness to invest). Therefore, I present the last hypothesis:

**H6:** Perceptions of audit quality are positively associated with willingness to invest.

### 2.3 Research Method

#### 2.3.1 Participants

Participants are 106 M.B.A. and executive M.B.A. students at a major public university. On average, participants are 31 years old with 9.1 years of work experience. Close to 52 percent of participants are female and 15 percent are executive M.B.A.s. On average, participants have taken 3.8 accounting and finance courses and have purchased or sold individual stock or mutual funds 19.3 times. Thus, the participants are appropriate proxies for nonprofessional investors. Further, 100 (95) percent of participants have made online (in-department store) purchases in the last three months and close to 47 percent of the participants have experienced online fraud or identity theft in the past. Participants were randomly assigned across experimental conditions and spent on average 12.85 minutes on the experiment. Twelve (out of 106) participants that failed one or both of the manipulation check questions are included in my analyses as the results remain qualitatively similar if the participants are excluded.

#### 2.3.2 Experimental Task and Design

I conduct an experiment using a 2 x 2 between-participant design and manipulate (1) cybersecurity examination provisioning type as joint or separate and (2) subsequent

---

7 Institutional Review Board approval was obtained prior to recruiting participants and collecting data.
8 Participants in the four experimental conditions do not vary significantly along any of the demographic factors. As a robustness check, I include all demographic factors, including investment experience and whether the participant is an M.B.A. or executive M.B.A. student, as covariates in my analyses, yielding qualitatively similar results.
cybersecurity incident as cybersecurity incident absent or present following the cybersecurity risk management examination disclosure. The experiment is administered online through the Qualtrics software. In step one, participants are presented with general background information about a fictitious company and a brief overview of stock and performance information, including sales, earnings, and analyst expectations. The financial information is designed to be perceived as positive. The participants are also provided information about the audit engagement, including the clean audit opinion and background information about the auditors. The retail industry setting is held constant. Comprehension check questions are used to ensure that participants attend to and understand the background information. Participants are then asked to provide initial valuation judgments about investment attractiveness and investment likelihood.

In step two of the experiment, the participants are first presented with information about the company’s decision to disclose information about their cybersecurity risk management program, the decision to hire an independent auditor to provide a cybersecurity risk management examination, the disclosure, and the cybersecurity risk management examination report. The participants are randomly presented one of the four experimental conditions based on the two between-participant manipulations: (1) Joint Provision and No Cybersecurity Incident, (2) Separate Provision and No Cybersecurity Incident, (3) Joint Provision and Subsequent Cybersecurity Incident, and (4) Separate Provision and Subsequent Cybersecurity Incident. The cybersecurity examination provisioning type manipulation (joint or separate provisioning) is administered in this step. To make the manipulation salient, participants are explicitly told whether the service was performed by the existing integrated ICFR and financial statement auditors or by another Big 4 accounting firm. The subsequent cybersecurity incident manipulation is also administered in this step. In the no cybersecurity incident conditions, the
participants are explicitly told that, as of a particular date subsequent to the cybersecurity assurance report disclosure, no significant cybersecurity incident has occurred. In the cybersecurity incident conditions, participants are instead told that, on a particular date (the same date as in the no incident conditions) subsequent to the cybersecurity risk management examination disclosure, a significant cybersecurity incident occurred.

Participants are then asked to again provide valuation judgments about investment attractiveness and investment likelihood. Participants also answer questions related to their perceptions of competence, independence, and audit quality. In step three, participants answer post-experiment questions, including demographic and manipulation check questions.

2.3.3 Dependent Variable

Willingness to Invest. I draw on prior research (e.g., Koonce and Lipe 2010; Elliott et al. 2015; Asay et al. 2018) to create my valuation judgment measures. Specifically, I use participants’ willingness to invest in the fictitious company Cost Saver as my dependent variable. I measure willingness to invest based on the average of participants’ perceptions of investment attractiveness and investment likelihood. To measure investment attractiveness, I ask participants how attractive an investment in Cost Saver is on a 7-point Likert scale anchored on 1 (very unattractive) and 7 (very attractive). To measure investment likelihood, I ask participants, assuming they were given $10,000 to invest in the department store retail industry, how likely are they to invest a portion of this amount in Cost Saver on a 7-point Likert scale anchored on 1 (very unlikely) and 7 (very likely). I capture participants’ willingness to invest both before and after the experimental manipulations. To remove noise introduced by individual participant idiosyncrasies, I control for pre-manipulation willingness to invest by using the difference between the post-manipulation and pre-manipulation measures as the dependent variable, similar
to prior research (e.g., Smith 2012, Asay et al. 2018; Koonce, Leitter, and White 2018). A positive change in willingness to invest between the pre- and the post-manipulation measures indicates an increased willingness to invest. For ease of exposition, I refer to the change in willingness to invest simply as \textit{willingness to invest}.

\textbf{2.3.4 Other Measured Variables}

\textit{Perceptions of Independence.} I define auditor independence as “a mental state of objectivity and lack of bias (SEC 2001,1) and “acting with integrity and objectivity and being able to withstand pressure from management to infringe professional standards” (Beattie et al. 1999, 79).\footnote{This definition of auditor independence is consistent with the AICPA’s auditing standards stating: “The auditor's independence from the entity safeguards the auditor's ability to form an audit opinion without being affected by influences that might compromise that opinion. Independence enhances the auditor's ability to act with integrity, to be objective, and to maintain an attitude of professional skepticism. Independence implies an impartiality that recognizes an obligation to be fair not only to management and those charged with governance of an entity but also users of the financial statements who may rely upon the independent auditor's report” (AICPA 2016, 93).} Following Lowe et al. (1999), I measure perceptions of independence by asking participants how confident they are that the auditors acted independently when performing Cost Saver's financial statements and related internal controls audit, using a 7-point Likert scale anchored on 1 (No Confidence) and 7 (Extreme Confidence). I also provide a definition of auditor independence to the participants: auditors are independent when they act with integrity and objectivity, and without biases, and when they do not give in to pressure from management.

\textit{Perceptions of Competence.} I define competence as a construct consisting of knowledge and the ability to use this knowledge in a specific context (Bassellier et al. 2003). Competence is similar to professional judgment, which is defined by the AICPA’s auditing standards as “the application of relevant training, knowledge, and experience, within the context provided by auditing, accounting, and ethical standards, in making informed decisions about the courses of
action that are appropriate in the circumstances of the audit engagement.” (AICPA 2016, 86). I measure perceptions of competence by asking participants how confident they are in the auditors’ competence in Cost Saver’s financial statements and related internal controls audit, on a 7-point Likert scale anchored on 1 (No Confidence) and 7 (Extreme Confidence). I also provide a definition of auditor competence to the participants: Auditors are competent when they have relevant knowledge and the ability to use this knowledge in a specific auditing context.

**Perceptions of Audit Quality.** I develop my measure of perceptions of the quality of the integrated ICFR and financial statements audits based on Gaynor et al.’s (2016) definition of a high-quality audit as “…one that provides a higher level of assurance that the auditor obtained sufficient appropriate evidence that the financial statements faithfully represent the firm’s underlying economics” and a high-quality non-financial audit as “…one that is conducted in compliance with assurance standards and provides a greater level of assurance on the respective information opined” (5). Using 7-point Likert scales anchored on 1 (No Confidence) and 7 (Extreme Confidence), I ask participants how confident they are that sufficient evidence was obtained and used to support: (1) the auditors’ clean opinion that the financial statements faithfully represent Cost Saver’s underlying economics and (2) the auditors’ clean opinion that Cost Saver maintained effective internal controls over financial reporting (PCAOB 2007). I then combine these two measures for an overall measure of perceptions of the quality of the integrated ICFR and financial statements audits.

**2.3.5 Pilot Study**

Participants were non-professional investors recruited from Amazon’s Mechanical Turk (MTurk). Rennekamp (2012); Koonce, Miller, and Winchel (2015); Brasel, Doxey, Grenier

---

10 Institutional Review Board approval was obtained prior to recruiting participants and collecting data.
and Reffett (2016), Chen, Han, and Tan (2016), and Farrell, Grenier, and Leiby (2017) demonstrate the appropriateness of using Amazon’s Mechanical Turk participants in accounting experiments. I enforced strict qualification requirements, including MTurk human intelligence task (HIT) approval ratings greater than 98 percent on at least 5,000 approved HITs, participants located in the U.S., and no duplicate IP addresses. In order to incentivize effort and attention, I implemented a bonus payment structure as recommended by Buchheit, Doxey, Pollard, and Stinson (2018). Participants earning a bonus took an average of 10.86 minutes to complete the experiment. Close to 46 percent of participants were female and participants were on average 40 years old with 18.5 years of work experience. On average, participants had taken 2.2 accounting and finance courses and had purchased or sold individual stock or mutual funds 17 times. Thus, the participants were an appropriate proxy for non-professional investors. Participants had made an average of 4-6 online purchases and 4-6 in-department store purchases in the last three months and close to 28 percent of the participants had experienced online fraud or identity theft in the past.

In summary, the results of the first experiment using MTurk participants showed that joint provisioning had a negative effect on investor perceptions of independence, without a corresponding positive effect on investor perceptions of competence. I also found that the effect of a subsequent cybersecurity incident on investor perceptions of competence was significantly more negative for joint provisioning compared to separate provisioning. The results of the first experiment using MTurk participants also showed no statistical difference between investors’ willingness to invest between joint provisioning and separate provisioning of the cybersecurity risk management examination.
Based on feedback from several reviewers and lessons learned, I made a number of changes after the first experiment using MTurk participants. Namely, prior to collecting new data, I made changes to my manipulations to remove a potential priming effect, revised my hypothesized model based on a more coherent and integrated theoretical framework, and recruited M.B.A. and executive M.B.A. students with more investment experience than the MTurk participants to participate in a new experiment with a modified instrument.

2.4 Results

2.4.1 Descriptive Statistics

Table 2.1 presents summary statistics for willingness to invest and perceptions of competence, perceptions of independence, and perceptions of audit quality by condition as well as mean comparisons between conditions. Similar to prior research (e.g., Smith 2012, Asay et al. 2018; Koonce, Leitter, and White 2018), willingness to invest is the change between the pre- and the post-manipulation measures. A positive change in willingness to invest indicates an increased willingness to invest.\(^\text{11}\) Interestingly, comparisons of means indicate that in the absence of a subsequent cybersecurity incident, joint provisioning compared to separate provisioning has a negative effect on willingness to invest, (p<0.001), but a positive effect on perceptions of competence (p=0.077). Comparisons of means also indicate that in the presence of a cybersecurity incident, joint provisioning compared to separate provisioning has a negative effect on perceptions of independence (p=0.026) and perceptions of audit quality (p=0.082). Additionally, comparisons of means indicate that a cybersecurity incident has a negative effect on willingness to invest for both joint provisioning and separate provisioning (p<0.001 and

\(^{11}\) Results from alternative analyses using the post-manipulation measure as the dependent variable and the pre-manipulation measure as a covariate for hypotheses testing are qualitatively similar.
p<0.001), and a negative effect on perceptions of competence (p<0.001); perceptions of independence (p=0.001), and perceptions audit quality (p=0.005), but only for joint provisioning.

2.4.2 Tests of Hypotheses

Due to the strong opportunity for knowledge spillover effects and increased auditor competence, H1 predicts that in the absence of a cybersecurity incident, investors will be more willing to invest when the cybersecurity risk management examination is jointly provisioned compared to separately provisioned. As shown in the ANOVA results in Table 2.2, investors are significantly less willing to invest when the cybersecurity risk management examination is jointly provisioned compared to separately provisioned (p=0.050; two-tailed), in the opposite direction as my prediction. I explore this surprising result further when I test the links in my hypothesized model shown in Figure 2.1.

H2a predicts that a subsequent cybersecurity incident will have a negative effect on willingness to invest and H2b predicts that a subsequent cybersecurity incident will also have a negative effect on the relation between joint provisioning and willingness to invest because a subsequent cybersecurity incident will reduce investors’ perceptions of auditor independence and competence when the services are jointly provisioned. As shown in the ANOVA results in Table 2.2, although I find a significant negative effect of a cybersecurity incident on willingness to invest (p<0.001), I do not find a significant interaction (p=0.271). It is possible that because investors already perceived joint provisioning as negative, the negative signal from a cybersecurity incident did not further reduce investors’ perceptions of auditor independence and competence under joint provisioning compared to under separate provisioning.

I next test my hypothesized model (H3 - H6) using PROCESS (Hayes 2018). The results of the model tests are provided in Table 2.3 and depicted in Figure 2.2.
Due to the strong opportunity for knowledge spillover effects and increased auditor competence, H3a predicts that in the absence of a cybersecurity incident, perceptions of competence will be greater when the cybersecurity risk management examination is jointly provisioned compared to separately provisioned. As hypothesized, the results indicate that in the absence of a cybersecurity incident, investors’ perceptions of auditor competence are more positive when the cybersecurity risk management examination is jointly provisioned compared to separately provisioned (p=0.047). I also find support for the prediction in H4a that a subsequent cybersecurity incident has a negative effect on the relation between provisioning type and perceptions of competence (p=0.020). The interaction suggests that when the cybersecurity risk management examination is jointly provisioned, the negative signal of a subsequent cybersecurity incident reverses investors’ positive perceptions of competence.

I do not find support for H3b, which predicts that in the absence of a cybersecurity incident, perceptions of auditor independence are lower when the cybersecurity risk management examination is jointly provisioned compared to separately provisioned (p=0.469). Absent a cybersecurity incident, it appears that perceptions of independence, typically theorized to explain why joint provisioning of non-audit services negatively affects perceptions of audit quality, does not explain why investors are less willing to invest when the cybersecurity risk management examination is jointly provisioned compared to separately provisioned.

I do, however, find support for H4b, which predicts that a subsequent cybersecurity incident has a negative effect on the relation between provisioning type and perceptions of independence (p=0.043). Further analysis indicates that when a cybersecurity incident is reported, the effect of joint provisioning on investor perceptions of independence is negative.
suggesting that investors are more sensitive to independence impairment concerns from joint provisioning in the event of a subsequent cybersecurity incident.

The results also support H5a and H5b predicting that perceptions of competence and perceptions of independence are positively associated with perceptions of audit quality (p<0.001 and p<0.001), and H6 predicting that perceptions of audit quality are positively associated with willingness to invest (p<0.001).

2.4.3 Summary of Results

Table 2.4 provides a summary of my results. The results show that in the absence of a subsequent cybersecurity incident investors are less willing to invest when the cybersecurity risk management examination in jointly provisioned compared to separately provisioned (contrary to H1). The results also show that a subsequent cybersecurity incident has a negative impact on willingness to invest (H2a supported), but does not have a significant negative effect on the relation between provisioning type and willingness to invest (H2b not supported).

I next explore whether my hypothesized model can help explain some surprising results. In the absence of a subsequent cybersecurity incident, joint provisioning has a positive effect on investors’ perceptions of auditor competence (H3a supported), but no significant effect on perceptions of auditor independence (H3b not supported). Interestingly, the negative signal of a subsequent cybersecurity incident reverses investors’ positive perceptions of competence (H4a supported) and increases investors’ sensitivity to potential independence impairments (H4b supported). Further, perceptions of competence and perceptions of independence have positive effects on perceptions of audit quality (H5a and H5b supported) which in turn has a positive effect on willingness to invest (H6 supported). Although the hypothesized model I developed based on theory is largely supported by my results, it appears that investors’ willingness to invest...
is also driven by factors not captured in my model. My results suggest that the competing effects of competence and independence typically theorized to explain the effect of joint provisioning on various proxies of audit quality used in the non-audit services literature may not completely explain nonprofessional investors’ judgment and decision making, at least in the context of cybersecurity non-audit services.

2.5 Conclusion

In response to increased cybersecurity risks and the growing demand for information about organizations’ cybersecurity risk management programs, the AICPA recently released a cybersecurity risk management examination service designed to provide external assurance related to the effectiveness of organization’s cybersecurity controls (AICPA 2017a). I report the results of an experiment designed to respond to the AICPA’s call for research that explores how users respond to cybersecurity risk management examination reporting (AAA 2017a; 2017b). My study is also motivated by recently expressed concerns by the SEC about cybersecurity threats facing nonprofessional (retail) investors and the need for more robust cybersecurity disclosures, including more information about organizations’ cybersecurity risk management programs and preventative actions taken to reduce and manage cybersecurity risk (SEC 2017b, 2018a).

Consistent with the theoretical argument that joint provisioning of the cybersecurity risk management examination creates a strong opportunity for increased auditor competence from knowledge spillover effects, my results indicate that in the absence of a cybersecurity incident, investors’ perceptions of competence are greater when the cybersecurity risk management examination is jointly compared to separately provisioned. I also find that when the cybersecurity risk management examination is jointly provisioned, the negative signal of a
subsequent cybersecurity incident reverses investors’ positive perceptions of competence and increase investors’ sensitivity to potential independence impairments. My results also indicate that investors are more willing to invest when the cybersecurity risk management examination is separately provisioned compared to jointly provisioned.

This study makes three contributions. First, I contribute to the growing literature related to cybersecurity. Most of this work has been archival in nature and as such, has not been able to examine the effects of the AICPA’s new cybersecurity risk management examination reporting and the AICPA’s call for research that explores how users respond to cybersecurity risk management examination reporting (AAA 2017a, 2017b). Using an experimental method, I am able to examine a potentially important implication of how cybersecurity risk management examinations are provisioned. Specifically, I find that investors are less willing to invest when the cybersecurity risk management examination is jointly provisioned compared to separately provisioned.

Second, this paper contributes to the research stream on non-audit services by not only examining investor perceptions of joint provisioning of cybersecurity risk management examinations, a unique and emerging non-audit service not previously examined, but also by providing insights into the longstanding debate over the theorized competing (i.e., suppressing) effects of increased competence and decreased independence on audit quality. Schneider et al. (2006) highlight that future research should focus on specific types of non-audit services rather than the broad and varying non-audit services fee categories used in many prior studies providing mixed results. In the absence of a subsequent cybersecurity incident, I find that joint provisioning has a positive effect on investors’ perceptions of auditor competence, but no significant effect on perceptions of auditor independence. Interestingly, the negative signal of a
subsequent cybersecurity incident reverses investors’ positive perceptions of competence and increases investors’ sensitivity to potential independence impairments. In other words, the effect of joint provisioning can have either positive or negative effects on perceptions of competence and either no significant effect or a negative effect on perceptions of independence depending on whether a negative signal of the quality of the non-audit service is present. Further, as predicted by theory, both perceptions of competence and perceptions of independence have positive effects on perceptions of audit quality. These results not only contribute to the non-audit services literature by showing how non-audit services are perceived differently depending on whether a negative signal of non-audit service quality is present, but the results also highlight the importance of measuring perceptions of independence and competence when examining how non-audit services affect perceptions of audit quality.

Third, this study contributes to purchasers of cybersecurity risk management examinations and informs regulators and standard setters by examining investors’ reactions to the AICPA’s recently adopted voluntary cybersecurity risk management examination reporting. My results indicate that it might be advantageous for purchasers of cybersecurity risk management examinations to provision the cybersecurity risk management examination separately from the audit due to the negative effect of joint provisioning on investors’ willingness to invest - an important finding given that cybersecurity has become a top concern for public companies and their boards (NACD 2017) who are looking to their financial statement auditors to provide cybersecurity services both within and outside the scope of the integrated ICFR and financial statements audits (AAA 2019).

My findings also provide insights to regulators and standard setters considering changes to the voluntary nature and provisioning guidelines of cybersecurity risk management
examinations. The PCAOB has emphasized the importance of auditors increasingly considering components of cybersecurity in the integrated ICFR and financial statements audits (PCAOB 2016, 2018) and public company auditors are concerned about investors’ increased expectations of the responsibilities of the audit firm in addressing cybersecurity risk (McKenna 2018; AAA 2019). At the same time, the PCAOB has also raised concerns that the rise of non-audit services, including cybersecurity services, is threatening auditor independence and increasing risks to nonprofessional investors (PCAOB 2014). Similar independence concerns related to non-audit services are being raised by regulators in the UK (CMA 2018). Moreover, the proposed law H.R.5069 (2016), the Cybersecurity Systems and Risks Reporting Act of 2016, has been introduced to amend the Sarbanes-Oxley Act of 2002 and related SEC oversight to also apply to cybersecurity systems and cybersecurity systems officers. Yet, my findings suggest that despite investors’ perceptions of increased competence consistent with knowledge spillover effects, in the event of a subsequent cybersecurity incident investors’ perceptions of audit quality is reduced when the cybersecurity risk management examination is performed jointly. Given that cybersecurity incidents are common and can occur despite clean opinions from high quality cybersecurity risk management examinations, the increasing focus by regulators on cybersecurity controls in integrated ICFR and financial statements audits may have unforeseen negative effects, especially on nonprofessional investors that may misinterpret this less than perfect signal of audit quality.

These observations should be interpreted in light of certain limitations, which also provide opportunities for future research. First, similar to other nonprofessional investor experimental studies, participants in my study have a limited set of information compared to when investors make actual investment decisions, limiting the generalizability of the results.
Future research could examine whether professional investors react differently than nonprofessional investors to cybersecurity risk management examination and cybersecurity incident disclosures. Second, I hold the retail industry constant in my study to control for industry effects and make the setting more salient to the participants. Future research could examine whether cybersecurity risk management examination and cybersecurity incident disclosures impact investors’ perceptions and decisions differently by industry. Third, I do not examine the perceived value of the AICPA’s new cybersecurity risk management examination compared to alternative cybersecurity assurance services available in the current voluntary and non-standardized cybersecurity assurance market and recommend that future research address this important question. Fourth, although not within the scope of this study, future research could also examine investors’ perceptions of CPAs’ expertise in the context of cybersecurity risk management examinations.

Finally, although the hypothesized model I developed based on theory is largely supported by my results, it appears that other non-modeled factors are also impacting investors’ willingness to invest. My results suggest that the competing effects of competence and independence, typically theorized to explain the results of the net effects of joint provisioning on various proxies of audit quality used in the non-audit services literature may not completely explain nonprofessional investors’ judgment and decision making in the context of cybersecurity non-audit services in particular and non-audit services in general, providing another opportunity for future research.
### 2.6 Tables for Essay 1

#### Table 2.1: Essay 1 Descriptive Statistics – Mean (Standard Deviation)

<table>
<thead>
<tr>
<th>Provisioning Type</th>
<th>Subsequent Cybersecurity Incident</th>
<th>Mean Comparison</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No Incident</td>
<td>Incident</td>
<td>Row Means</td>
</tr>
<tr>
<td><strong>Joint</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willingness to Invest</td>
<td>-0.250 (0.752)</td>
<td>-2.056 (1.565)</td>
<td>-1.170 (1.525)</td>
</tr>
<tr>
<td>Perceived Competence</td>
<td>5.731 (1.002)</td>
<td>4.370 (1.305)</td>
<td>5.038 (1.344)</td>
</tr>
<tr>
<td>Perceived Independence</td>
<td>5.269 (1.251)</td>
<td>4.037 (1.372)</td>
<td>4.642 (1.442)</td>
</tr>
<tr>
<td>Perceived Audit Quality</td>
<td>5.231 (1.125)</td>
<td>4.241 (1.310)</td>
<td>4.726 (1.310)</td>
</tr>
<tr>
<td>n = 26</td>
<td>n = 27</td>
<td>n = 53</td>
<td></td>
</tr>
<tr>
<td><strong>Separate</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willingness to Invest</td>
<td>0.463 (0.587)</td>
<td>-1.654 (1.880)</td>
<td>-0.575 (1.736)</td>
</tr>
<tr>
<td>Perceived Competence</td>
<td>5.148 (1.322)</td>
<td>4.808 (1.357)</td>
<td>4.981 (1.337)</td>
</tr>
<tr>
<td>Perceived Independence</td>
<td>5.296 (0.993)</td>
<td>4.923 (1.440)</td>
<td>5.113 (1.235)</td>
</tr>
<tr>
<td>Perceived Audit Quality</td>
<td>5.111 (0.923)</td>
<td>4.885 (1.329)</td>
<td>5.000 (1.135)</td>
</tr>
<tr>
<td>n = 27</td>
<td>n = 26</td>
<td>n = 53</td>
<td></td>
</tr>
<tr>
<td><strong>Column Means</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willingness to Invest</td>
<td>0.113 (0.757)</td>
<td>-1.858 (1.722)</td>
<td>-0.873 (1.653)</td>
</tr>
<tr>
<td>Perceived Competence</td>
<td>5.434 (1.201)</td>
<td>4.585 (1.336)</td>
<td>5.009 (1.334)</td>
</tr>
<tr>
<td>Perceived Independence</td>
<td>5.283 (1.116)</td>
<td>4.472 (1.462)</td>
<td>4.877 (1.357)</td>
</tr>
<tr>
<td>Perceived Audit Quality</td>
<td>5.170 (1.019)</td>
<td>4.557 (1.347)</td>
<td>4.863 (1.228)</td>
</tr>
<tr>
<td>n = 53</td>
<td>n = 53</td>
<td>n = 106</td>
<td></td>
</tr>
<tr>
<td><strong>Grand Means</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willingness to Invest</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived Competence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived Independence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived Audit Quality</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>p-value</td>
<td>&lt;0.001</td>
<td>0.401</td>
<td></td>
</tr>
<tr>
<td>Perceived Competence</td>
<td>0.077</td>
<td>0.237</td>
<td></td>
</tr>
<tr>
<td>Perceived Independence</td>
<td>0.931</td>
<td>0.026</td>
<td></td>
</tr>
<tr>
<td>Perceived Audit Quality</td>
<td>0.673</td>
<td>0.082</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** All p-values are reported two-tailed. *Provisioning Type* is manipulated as joint or separate provisioning of the cybersecurity examination and the integrated ICFR and financial statements audits (joint=1; separate=0). *Cybersecurity Incident* is manipulated as the presence or absence of a reported cybersecurity incident subsequent to the cybersecurity examination report date (incident=1; no incident=0). *Willingness to Invest* is the change between the pre- and the post-manipulation measures. A positive change in *Willingness to Invest* indicates an increased willingness to invest. *Willingness to Invest* includes investment attractiveness and investment likelihood. Participants rate investment attractiveness on a seven-point scale with endpoints “very unattractive” and “very attractive.” Participants rate investment likelihood on a seven-point scale with endpoints “very unlikely” and “very likely.” Participants rate their confidence in the audit firm’s (1) *Independence*, (2) *Competence*, and (3) *Audit Quality* on seven-point scales with endpoints “No Confidence” and “Extreme Confidence.”
Table 2.2: The Effect of Provisioning Type and Cybersecurity Incident on Willingness to Invest

Panel A: ANOVA

<table>
<thead>
<tr>
<th>Source</th>
<th>df</th>
<th>MS</th>
<th>F</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Type</td>
<td>1</td>
<td>8.229</td>
<td>4.792</td>
<td>0.031</td>
</tr>
<tr>
<td>Cybersecurity Incident (H2a)</td>
<td>1</td>
<td>101.889</td>
<td>59.340</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>Provisioning Type X Cybersecurity Incident (H2b)</td>
<td>1</td>
<td>0.642</td>
<td>0.374</td>
<td>0.271</td>
</tr>
<tr>
<td>Error</td>
<td>102</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Panel B: Planned Comparison

<table>
<thead>
<tr>
<th>Relation</th>
<th>df</th>
<th>F-stat</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separate &gt; Joint for No Incident (H1)</td>
<td>1</td>
<td>3.921</td>
<td>0.050*</td>
</tr>
</tbody>
</table>

Notes: P-values are reported one-tailed when the path coefficient is in the expected direction, otherwise two-tailed. Provisioning Type is manipulated as joint or separate provisioning of the cybersecurity examination and the integrated ICFR and financial statements audits. Cybersecurity Incident is manipulated as the presence or absence of a reported cybersecurity incident subsequent to the cybersecurity examination report date. Willingness to Invest is the change between the pre- and the post-manipulation measures. A positive change in Willingness to Invest indicates an increased willingness to invest. Willingness to Invest includes investment attractiveness and investment likelihood. Participants rate investment attractiveness on a seven-point scale with endpoints “very unattractive” and “very attractive.” Participants rate investment likelihood on a seven-point scale with endpoints “very unlikely” and “very likely.”

*Result is significant in the opposite direction as predicted, two-tailed.
Table 2.3: Results of Hypothesized Model

<table>
<thead>
<tr>
<th>Path</th>
<th>Coefficient</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Type → Perceived Competence (H3a)</td>
<td>0.583</td>
<td>0.047</td>
</tr>
<tr>
<td>Provisioning Type → Perceived Independence (H3b)</td>
<td>-0.027</td>
<td>0.469</td>
</tr>
<tr>
<td>Provisioning Type and Cybersecurity Incident Interaction → Perceived Competence (H4a)</td>
<td>-1.020</td>
<td>0.020</td>
</tr>
<tr>
<td>Provisioning Type and Cybersecurity Incident Interaction → Perceived Independence (H4b)</td>
<td>-0.859</td>
<td>0.043</td>
</tr>
<tr>
<td>Perceived Competence → Perceived Audit Quality (H5a)</td>
<td>0.437</td>
<td>&lt;0.001</td>
</tr>
<tr>
<td>Perceived Independence → Perceived Audit Quality (H5b)</td>
<td>0.401</td>
<td>&lt;0.001</td>
</tr>
<tr>
<td>Perceived Audit Quality → Willingness to Invest (H6)</td>
<td>0.384</td>
<td>&lt;0.001</td>
</tr>
</tbody>
</table>

Notes: P-values are reported one-tailed when the path coefficient is in the expected direction, otherwise two-tailed.

Provisioning Type is manipulated as joint or separate provisioning of the cybersecurity examination and the integrated ICFR and financial statements audits (joint=1; separate=0). Cybersecurity Incident is manipulated as the presence or absence of a reported cybersecurity incident subsequent to the cybersecurity examination report date (incident=1; no incident=0). Willingness to Invest is the change between the pre- and the post-manipulation measures. A positive change in Willingness to Invest indicates an increased willingness to invest. Willingness to Invest includes investment attractiveness and investment likelihood. Participants rate investment attractiveness on a seven-point scale with endpoints “very unattractive” and “very attractive.” Participants rate investment likelihood on a seven-point scale with endpoints “very unlikely” and “very likely.” Participants rate their confidence in the audit firm’s (1) Independence, (2) Competence, and (3) Audit Quality on seven-point scales with endpoints “No Confidence” and “Extreme Confidence.”
<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>p-value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1: In the absence of a cybersecurity incident, investors will be more</td>
<td>0.050</td>
<td>Not Supported*</td>
</tr>
<tr>
<td>willing to invest when the cybersecurity examination is jointly compared to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>separately provisioned.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H2a: A subsequent cybersecurity incident will negatively impact</td>
<td>&lt; 0.001</td>
<td>Supported</td>
</tr>
<tr>
<td>willingness to invest.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H2b: A subsequent cybersecurity incident will have a negative effect on</td>
<td>0.271</td>
<td>Not Supported</td>
</tr>
<tr>
<td>the relation between provision type and willingness to invest.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H3a: In the absence of a cybersecurity incident, perceptions of</td>
<td>0.047</td>
<td>Supported</td>
</tr>
<tr>
<td>competence will be greater when the cybersecurity examination is jointly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>compared to separately provisioned.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H3b: In the absence of a cybersecurity incident, perceptions of</td>
<td>0.469</td>
<td>Not Supported</td>
</tr>
<tr>
<td>independence will be lower when the cybersecurity examination is jointly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>compared to separately provisioned.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H4a: A cybersecurity incident will have a negative effect on the relation</td>
<td>0.020</td>
<td>Supported</td>
</tr>
<tr>
<td>between provision type and investors’ perceptions of auditor competence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H4b: A cybersecurity incident will have a negative effect on the relation</td>
<td>0.043</td>
<td>Supported</td>
</tr>
<tr>
<td>between provision type and investors’ perceptions of auditor independence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H5a: Perceptions of competence are positively associated with perceptions</td>
<td>&lt;0.001</td>
<td>Supported</td>
</tr>
<tr>
<td>of audit quality.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H5b: Perceptions of independence are positively associated with</td>
<td>&lt;0.001</td>
<td>Supported</td>
</tr>
<tr>
<td>perceptions of audit quality.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H6: Perceptions of audit quality are positively associated with</td>
<td>&lt;0.001</td>
<td>Supported</td>
</tr>
<tr>
<td>willingness to invest.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** P-values are reported one-tailed when the path coefficient is in the expected direction, otherwise two-tailed.

*Result is significant in the opposite direction as predicted, two-tailed.
2.7 Figures for Essay 1

Figure 2.1: Hypothesized Model
Figure 2.2: Hypotheses Results with Path Coefficients (p-values)

Notes: All p-values are reported one-tailed. Analyses are performed using PROCESS (Hayes 2018) with 5,000 bootstrap samples and 95% level of confidence. Provisioning Type is manipulated as joint or separate provisioning of the cybersecurity examination and the integrated ICFR and financial statements audits (joint=1; separate=0). Cybersecurity Incident is manipulated as the presence or absence of a reported cybersecurity incident subsequent to the cybersecurity examination report date (incident=1; no incident=0). Willingness to Invest is the change between the pre- and the post-manipulation measures. A positive change in Willingness to Invest indicates an increased willingness to invest. Willingness to Invest includes investment attractiveness and investment likelihood. Participants rate investment attractiveness on a seven-point scale with endpoints “very unattractive” and “very attractive.” Participants rate investment likelihood on a seven-point scale with endpoints “very unlikely” and “very likely.” Participants rate their confidence in the audit firm’s (1) Independence, (2) Competence, and (3) Audit Quality on seven-point scales with endpoints “No Confidence” and “Extreme Confidence.”
Chapter 3. Essay 2: The Impact of the Type of Cybersecurity Assurance Service and Cybersecurity Incidents on Investor Perceptions and Decisions

2.8 Introduction

As the Securities and Exchange Commission (SEC) noted recently, “Cybersecurity is critical to the operations of our markets and the risks are significant” (SEC 2017a, 1). Cybercrime can result in reputational damage, loss of proprietary information, revenue loss, government fines, litigation expenses, increased insurance premiums, and incident response and mitigation expenses (SEC 2018a; CAQ 2016). With the goal of providing more complete and useful information to investors, the SEC recently issued guidance for public company cybersecurity disclosures highlighting the importance of information about organizations’ cybersecurity risk management programs and “…the adequacy of preventative actions taken to reduce cybersecurity risks” (SEC 2018a, 14).

In response to heightened attention to cybersecurity risk, the American Institute of Certified Public Accountants (AICPA) has released a new examination service designed to provide external assurance for organizations’ cybersecurity risk management programs (AICPA 2017a, 2018). The cybersecurity risk management examination is a voluntary, general-use report that is intended to benefit a broad range of potential users including investors and other stakeholders such as customers, analysts, directors, business partners, and regulators (AICPA 2017b, 207).
The top six audit firms are currently advertising their cybersecurity risk management examination service offerings and public company boards are increasingly requesting cybersecurity assurance services (Deloitte 2018a; AAA 2019).

The current voluntary cybersecurity assurance reporting market includes many alternative third-party assurance services and providers (Kuranda 2017) and disparate assurance programs and frameworks with no widely accepted standard (AICPA 2017a). For example, cybersecurity assurance services can differ in terms of the comprehensiveness of the subject matter (AICPA 2017b). A more comprehensive cybersecurity risk management examination includes all components of a cybersecurity risk management program such as the nature of business operations and information at risk, cybersecurity objectives, risk assessments, governance structure, communications, monitoring, and control processes (AICPA 2017b). Each component further consists of a number of controls that are examined. For example, vulnerability and penetration tests are included as a single control within the monitoring and risk assessment component of a cybersecurity risk management program (AICPA 2017b). Yet, vulnerability and penetration tests are offered by various vendors as a standalone service. Stakeholders may have difficulty distinguishing between the comprehensiveness of alternative cybersecurity assurance services and may even perceive a vulnerability and penetration test as equally or perhaps more valuable than a cybersecurity risk management examination. Moreover, prior research examining another AICPA IT-related voluntary assurance reporting initiative called WebTrust that did not gain any significant market acceptance find that information users do not recognize

---

13 System and Organization Controls (SOC) for Cybersecurity examinations include three components: (1) management’s description of the cybersecurity risk management program, (2) management’s assertion that the description is presented in accordance with the description criteria and that the controls within the program were effective based on the control criteria, and (3) the CPA’s opinion on management’s description and the effectiveness of the controls within the program (AICPA 2017a).
the value of the more comprehensive external assurance services relative to less comprehensive 
external assurance alternatives (Mauldin and Arunachalam 2002; Gendron and Barrett 2004). Accordingly, the first objective of this study is to examine the impact of the type of voluntary 
external cybersecurity assurance service on investors’ perceptions and decisions.

Cybersecurity incidents are increasingly prevalent and “no company or organization is 
immune from cyberattack” (SEC 2018b, 1). The average cost of cybercrime has increased 62 
percent over the last five years and cybercrime continues to become more sophisticated 
(Accenture 2017). In the context of cybersecurity assurance disclosures, previous cybersecurity 
incidents are likely to affect investors’ perceptions of the importance of the type of external 
assurance provided and in turn investors’ perceptions and decisions. More specifically, if a 
cybersecurity incident precedes the external cybersecurity assurance (i.e., obtaining the 
cybersecurity external assurance is in response to a significant cybersecurity incident), investors 
may view the cybersecurity assurance service as a post-hoc reactive measure and may therefore 
be more sensitive to the type of external assurance service provided. In the presence of a 
previous cybersecurity incident, a more comprehensive cybersecurity assurance service might 
increase investors’ perceptions of the company’s ability to not only prevent future cybersecurity 
incidents, but also to recover from future cybersecurity incidents that are not prevented.14 
Therefore, the second objective of this study is to examine the effect of a previous cybersecurity 
incident on the relation between the type of cybersecurity assurance service and investors’ 
perceptions and decisions.

---

14 SEC Chairman Clayton underscores the importance of both preventive and reactive measures to reduce 
cybersecurity risk and states that “we also must recognize...that there will be intrusions, and that a key component 
of cyber risk management is resilience and recovery.” (SEC 2017a, 1)
I draw on dual processing theories (Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003), the management disclosure credibility framework (Mercer 2004), and the information hypothesis (Wallace 1987) to develop hypotheses regarding the impact of the type of cybersecurity assurance service on investors’ willingness to invest, the potential positive moderating effect of a previous cybersecurity incident, and the potential mediating effect of perceptions of cybersecurity assurance services quality. To test my hypotheses, I conduct an experiment using a 2 x 2 between-participant design, in which I manipulate type of cybersecurity assurance service as a more comprehensive cybersecurity risk management examination or a less comprehensive vulnerability and penetration test and cybersecurity incident as no incident or incident precedes assurance. I measure the effect of these manipulations on willingness to invest, perceptions of cybersecurity assurance services quality, and perceptions of management credibility.

Participants in the study are nonprofessional (i.e., retail) investors because the SEC is concerned about the “risks to retail investors in today’s marketplace” (SEC 2017b) and “protecting retail investors is at the heart of the Commission’s mission” (SEC 2018c). The importance of examining nonprofessional investors’ perceptions of cybersecurity assurance disclosures is underscored by the SEC’s concern for the grave cybersecurity threats facing the “investing public” and the need for more robust cybersecurity disclosures (SEC 2018a, 2). In addition, cybersecurity incidents involving the theft of sensitive customer information are often highly publicized leading to nonprofessional investors’ heightened awareness of cybersecurity risk.15 Nonprofessional investors’ awareness of cybersecurity risk is further heightened as their

---

15 Cybersecurity incidents are increasing in both numbers and economic significance and are required to be disclosed if material (SEC 2011, 2018a).
personal information and devices are increasingly digitally connected and susceptible to cybersecurity threats (e.g., NCSA 2017; SEC 2017c).

I find that investors are more willing to invest when management disclosures describe a more comprehensive cybersecurity risk management examination rather than a less comprehensive vulnerability and penetration test. This result is significant both in the absence of a cybersecurity incident and when a cybersecurity incident precedes cybersecurity assurance. I also find that investors’ perceptions of cybersecurity assurance services quality mediate the relation between type of cybersecurity assurance service and willingness to invest. Additional analyses suggest that a more comprehensive assurance service results in higher perceptions of cybersecurity assurance services quality because of the perception that the company is more prepared to recover from future cybersecurity incidents that are not prevented. The results also show that higher perceptions of cybersecurity assurance services quality have a positive effect on investor perceptions of management credibility, which in turn has a positive effect on willingness to invest.

This study makes three contributions to research and practice. First, I contribute to the growing literature related to cybersecurity disclosures. Using an experimental method, I am able to examine the effect of the AICPA’s new cybersecurity risk management examination in comparison to competing external assurance services on investors’ perceptions of cybersecurity assurance service quality and answer the AICPA’s call for research on how users react to cybersecurity assurance reporting (AAA 2017a, 2017b). I also shed light on investors’ perceptions of important aspects of cybersecurity risk management assurance in terms of a company’s ability to not only prevent future cybersecurity incidents, but also to recover from future cybersecurity incidents that are not prevented.
Second, I contribute to the voluntary assurance disclosure literature by examining investor reactions to management disclosures of alternative types of voluntary external cybersecurity assurance service, beyond a comparison of the absence or presence of external assurance reports provided by CPAs previously examined in other non-financial voluntary assurance settings. My results show that the comprehensiveness of the voluntary assurance service disclosed by management affects users’ judgments and decisions. I also find that management’s choice to acquire a more comprehensive cybersecurity assurance service has a positive effect on investors’ perceptions of management credibility, which in turn has a positive effect on investors’ willingness to invest.

Third, this study makes an important contribution to practice. The new cybersecurity risk management examination service shares many features with the WebTrust service that did not gain much traction in the market. For example, both WebTrust and cybersecurity risk management examinations are designed and promoted by the AICPA as a voluntary assurance service over IT related controls and face competition from less comprehensive and less costly assurance service alternatives in a voluntary and non-standardized assurance market. However, despite the limited success of WebTrust, my results suggest that nonprofessional investors are sensitive to the type of cybersecurity assurance service provided, and companies can benefit from investing in more comprehensive cybersecurity risk management assurance services. This is an important finding given that cybersecurity has become a top concern for public companies and their boards who are increasingly looking to CPA firms to provide cybersecurity assurance services (AICPA 2018; Deloitte 2018a; EY 2018; AAA 2019).
2.9 Theory and Hypotheses Development

3.2.1 External Assurance

Mercer’s (2004) management disclosure credibility framework explains that investors’ perceptions of external assurance, management credibility, and contextual factors together effect investors’ valuation judgments. Consistent with source credibility theory (Birnbaum and Stegner 1979) and the importance of the credibility of a message’s source, Mercer’s (2004) management disclosure credibility framework suggests that external assurance supporting a management disclosure affects investors’ perceptions of disclosure credibility and the extent to which investors rely on the disclosure for valuation judgments. For example, prior research finds that users perceive management disclosures with external assurance reports as more credible than management disclosures without external assurance reports (e.g., Libby 1979; Blackwell, Noland, and Winters 1998; Hodge 2001).

Based on Mercer’s (2004) management disclosure credibility framework and Wallace’s (1987) information hypothesis explaining that external assurance reduces information asymmetry and uncertainty, Coram, Monroe, and Woodliff (2009) find that the presence of an external assurance report is particularly important if financial statement users perceive management disclosures of non-financial information to be incentive-consistent (i.e., if the disclosure could be perceived as self-serving).16 Prior research examining voluntary corporate social responsibility reporting similarly finds that nonprofessional investors and financial analysts perceive managements’ incentive-consistent corporate social responsibility disclosures as more credible in the presence versus absence of external assurance reports (Pflugrath, Roebuck, and Simnett

---

16 Given the voluntary nature of cybersecurity external assurance disclosures, cybersecurity external assurance disclosures are unlikely to contain negative news and are likely to be perceived as incentive consistent.
This research also shows that the presence of external assurance reports has a positive effect on stock price assessments (Brown-Liburd and Zamora 2014) and willingness to invest (Cheng, Green, and Ko 2015). However, prior research has not examined the impact of the AICPA’s new cybersecurity risk management examination service in comparison to alternative voluntary assurance services available in the current voluntary and non-standardized cybersecurity assurance market.

Findings from prior literature examining an earlier AICPA IT-related voluntary assurance reporting initiative called WebTrust provide insights. In 1997, the AICPA launched WebTrust, a third-party web assurance seal for business-to-consumer e-commerce, as an opportunity to build on CPA’s expertise in audit and assurance (Elliott 1998; Gendron and Barrett 2004). Although WebTrust provided a significantly more comprehensive assurance service than alternative third-party web assurance seals such as TRUSTe (sponsored by IBM and Microsoft) and BBBOnLine (sponsored by the Better Business Bureau), WebTrust “failed to generate support in the marketplace” (Gendron and Barrett 2004, 563). The alternative services were not only less expensive and easier for management to obtain, but consumers were also not sensitive to the type of assurance service provided by the different web assurance seals and did not recognize the value provided by WebTrust in terms of being a more comprehensive assurance services (Mauldin and Arunachalam 2002; Gendron and Barrett 2004; Bahmanziari, Odom, and Ugrin 2009). Although the WebTrust service “largely failed” (Gendron and Barrett 2004, 594), its principles and criteria evolved and contributed to the current Trust Services Criteria used for SOC assurance services (AICPA 2018).

Similar to the voluntary e-commerce assurance market when WebTrust was launched, the current cybersecurity assurance market includes many alternative third-party assurance services
and providers (Kuranda 2017) and disparate cybersecurity assurance programs and frameworks with no widely accepted standard (AICPA 2017a). For example, cybersecurity assurance services can differ in terms of the comprehensiveness of the subject matter (AICPA 2017b). A more comprehensive cybersecurity risk management examination includes all components of a cybersecurity risk management program such as the nature of business operations and information at risk, cybersecurity objectives, risk assessments, governance structure, communications, monitoring, and control processes (AICPA 2017b). Each component further consists of a number of controls that are examined in the AICPA’s cybersecurity risk management examination. Vulnerability and penetration tests, for example, are included as a single control within the monitoring and risk assessment component of a cybersecurity risk management program (AICPA 2017b). However, less comprehensive vulnerability and penetration tests are offered by various vendors as a standalone service. In the context of cybersecurity, an investor may have difficulties in distinguishing the comprehensiveness of alternative services and may even perceive a vulnerability and penetration test as equally or perhaps more valuable than a cybersecurity risk management examination.

Although many similarities exist between the web assurance context and the cybersecurity assurance context in terms of alternative types of voluntary assurance services, one difference between the web assurance context and the cybersecurity assurance context is that consumers are protected by credit card security guarantees from fraudulent transactions when making online purchases (Mauldin and Arunachalam 2002; Kim, Steinfield, and Lai 2008). Consequently, although consumers’ private information is at risk, online consumers may be less sensitive to the type of assurance service provided relative to nonprofessional investors who are not protected from stock price declines. Another difference between the web assurance and
cybersecurity assurance contexts is that nonprofessional investors have a heightened awareness of cybersecurity risk because cybersecurity incidents involving the theft of sensitive customer information are often highly publicized and nonprofessional investors’ personal information and devices are increasingly digitally connected and susceptible to cybersecurity threats (e.g., SEC 2017c; 2018b). Given these distinctions, I expect that investors will differentiate between alternative cybersecurity assurance services that vary in terms of the comprehensiveness of the assurance service provided. Drawing again on Mercer’s (2004) management disclosure credibility framework and Wallace’s (1987) information hypothesis explained above, more comprehensive external assurance services will increase investors’ valuation judgments (e.g., willingness to invest). Accordingly, I present the following hypothesis:

**H1**: In the absence of a cybersecurity incident, investors are more willing to invest in the presence of a more compared to less comprehensive cybersecurity assurance service.

### 3.2.2 Cybersecurity Incidents

Cybersecurity incidents are increasing in both numbers and economic significance and are required to be disclosed if material (SEC 2011, 2018a). Prior archival research finds a negative market reaction to reported cybersecurity incidents (e.g., Campbell, Gordon, Loeb, and Zhou 2003; Goel and Shawky, 2009; Gatzlaff and McCullough, 2010; Hinz, Nofer, Schiereck, and Trillig 2015). In the context of cybersecurity disclosures, previous cybersecurity incidents are likely to also affect investors’ perceptions of the importance of the type of external assurance provided and in turn investors’ willingness to invest. More specifically, if a cybersecurity incident precedes the external cybersecurity assurance (i.e., obtaining the cybersecurity external assurance is in response to a significant cybersecurity incident), investors may be more sensitive to the type of external assurance provided and a more comprehensive assurance service might
increase investors’ perceptions of the company’s ability to not only prevent but also recover from future cybersecurity incidents. To support this conjecture, I draw on dual processing theories to explain how nonprofessional investors process types of external cybersecurity assurance services disclosures in the presence versus absence of a cybersecurity incident.

Dual processing theories differentiate between simple heuristic processing (i.e., peripheral route or system one processing) and effortful systematic processing (i.e., central route or system two processing) (Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003). In heuristic processing, individuals rely on easily accessible cues (e.g. source credibility) to reduce information processing demands when evaluating new information (Birnbaum and Stegner 1979; Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003). In systematic processing (i.e., central route or system two processing) individuals have the motivation and ability to use more effortful processing and are more likely to actively attend to the content of the information (i.e., message) being processed (Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003).

Contextual variables can influence individuals’ motivation to engage in effortful systematic processing beyond simple heuristic processing (Chaiken 1980; Petty and Cacioppo 1986; Chaiken and Maheswaran 1994; Kahneman 2003). Consistent with dual processing theories, prior research in accounting has found that contextual factors can motivate individuals to engage in effortful systematic processing for example in the context of auditor performance reviews (Brazel, Agoglia, and Hatfield 2004), performance-based contracts (Farrell, Goh, and White 2014), and auditing of complex estimates (Griffith 2018).

Applying dual processing theories to the cybersecurity disclosure setting, in the absence of a cybersecurity incident, nonprofessional investors are more likely to engage in simple
heuristic processing and rely primarily on easily accessible cues resulting in less sensitivity to the type of external cybersecurity assurance service. However, a contextual variable such as a cybersecurity incident can motivate investors to engage in effortful systematic processing resulting in increased attention to the information about the cybersecurity assurance service provided, including the details of the comprehensiveness of the cybersecurity assurance provided. Drawing again on Mercer’s (2004) management disclosure credibility framework and Wallace’s (1987) information hypothesis, more comprehensive external assurance services impact investors’ valuation judgments (e.g., willingness to invest). Based on this discussion, I present the following hypothesis:

H2: The difference between willingness to invest in the presence of more and less comprehensive cybersecurity assurance services will be greater when a cybersecurity incident precedes cybersecurity assurance than in the absence of an incident.

3.2.3 Perceptions of Cybersecurity Assurance Services Quality

As discussed earlier, Mercer’s (2004) disclosure credibility framework suggests that external assurance supporting a management disclosure affects investors’ perceptions of the credibility of management disclosures and in turn investors’ valuation judgments. Consistent with Mercer (2004), in order for the type of external cybersecurity assurance service to influence investors’ willingness to invest, investors must indeed perceive the external assurance service associated with the management disclosure to be of high assurance quality.

The experimental method provides an opportunity to directly measure investors’ perceptions of cybersecurity assurance services quality and to examine whether this important intervening variable explains why a particular relation exists. For example, Smith (2012) directly measures investors’ perceptions of audit quality and finds that this intervening variable mediates the relation between changes in auditing standards and investors’ investment allocations.
Gimbar, Hansen, and Ozlanski (2016) also measure perceptions of audit quality and find that jurors’ perceptions of audit quality mediate the relation between critical audit matters and auditor liability.

I expect that investors will perceive more comprehensive cybersecurity risk management examinations to be of higher cybersecurity assurance services quality than less comprehensive cybersecurity assurance services and that investors’ perceptions of cybersecurity assurance services quality will mediate the relation between the type of cybersecurity assurance service and willingness to invest both in the absence and presence of a prior cybersecurity incident.

Accordingly, I present the following mediation hypotheses:

**H3a:** Perceptions of cybersecurity assurance service quality will mediate the relation between the type of cybersecurity assurance service and willingness to invest in the absence of a cybersecurity incident.

**H3b:** Perceptions of cybersecurity assurance service quality will mediate the relation between the type of cybersecurity assurance service and willingness to invest when a cybersecurity incident precedes cybersecurity assurance.

### 2.10 Research Method

#### 3.3.1 Participants

Participants are 465 nonprofessional investors recruited from Amazon’s Mechanical Turk platform (MTurk). Rennekamp 2012; Konce, Miller, and Winchel (2015); Brasel, Doxey, Grenier and Reffett (2016), and Farrell, Grenier, and Leiby (2017) demonstrate the appropriateness of using MTurk participants in accounting experiments. I enforced strict qualification requirements, including a MTurk human intelligence task (HIT) approval rate greater than 98 percent on at least 5,000 approved HITs, no duplicate IP addresses, and participants located in the U.S. To incentivize effort and attention I also implement a bonus
payment structure as recommended by Buchheit, Doxey, Pollard, and Stinson (2018). I focus on nonprofessional (i.e., retail) investors’ perceptions of cybersecurity assurance disclosures because the SEC is concerned about the “risks to retail investors in today’s marketplace” (SEC 2017b) and the grave cybersecurity threats facing the “investing public” and the need for more robust cybersecurity disclosures (SEC 2018a, 2). The importance of nonprofessional (i.e., retail) investors’ perceptions is underscored by 44 percent of U.S. households (56 million households) owning mutual funds (SEC 2018d) and 52 percent of U.S. households owning stock (Federal Reserve 2017). These nonprofessional investors have a heightened awareness of cybersecurity risks because many cybersecurity incidents involving the theft of sensitive customer information are highly publicized (e.g., Equifax, Target, and Yahoo). Nonprofessional investors also have a heightened awareness of cybersecurity risks because their personal information and devices are increasingly digitally connected and susceptible to cybersecurity threats (e.g., NCSA 2017; SEC 2017c).

The participants are on average 37.5 years old with 15.9 years of work experience and 56.4 percent are male. On average, the participants have taken 2.0 accounting and finance courses and have purchased or sold individual stocks or mutual funds 17.3 times. Thus, the participants are an appropriate proxy for nonprofessional investors. Further, 91.2 (97.8) percent of participants report having have made in-store (online) department store purchases in the last three months and 33.1 percent of participants report having been a victim of identity theft or credit card fraud. On average, participants spent 6.34 minutes completing the experiment corresponding to a compensation of $9.26 per hour. In support of random assignment of participants to experimental conditions, multiple comparisons with Tukey HSD do not indicate

---

17 Institutional Review Board approval was obtained prior to recruiting participants and collecting data.
any significant between-group differences in terms of investment experience, accounting and finance courses, work experience, age, gender, time spent on the task, identity theft or credit card fraud, in-store purchases, and online purchases.18

3.3.2 Experimental Task and Design

The experiment employs a 2 x 2 between-participant design and manipulates type of cybersecurity assurance service as a more comprehensive cybersecurity risk management examination or a less comprehensive vulnerability and penetration test and cybersecurity incident as no incident or incident precedes assurance. The experiment is administered online through Qualtrics software. In step one, participants are informed of recent cybersecurity guidance from U.S. regulators including the SEC’s (2018a) guidance for public company cybersecurity disclosures and the new National Institute of Standards and Technology (NIST) Cybersecurity Framework developed under U.S. Executive Order 13636 and formalized by the U.S. Cybersecurity Enhancement Act of 2014 (NIST 2018). I provide this regulatory information to participants because although it is in the process of being widely publicized to nonprofessional investors in the popular press (e.g., Javers 2018; McKenna 2018; Pisani 2018; Schroeder and Finkle 2018; Shumsky 2018; Skroupa 2018; Stone 2018; Woods 2018) it is relatively new at the time of conducting the experiment.

Participants are then provided background information about a fictitious company, Cost Saver. The background information includes financial performance ratios and statistics for the company as well as corresponding industry averages. Participants are also provided information

---

18 Given that I did not detect significant between-group differences, the results reported are based on analyses without control variables. The results are qualitatively similar when the control variables are included in the models.
about the company’s e-commerce strategy. Comprehension check questions are used to assess whether participants attend to and understand the background information.

In step two of the experiment, participants are presented with management disclosures that describe the nature and timing of a cybersecurity incident and that Cost Saver obtained a cybersecurity assurance service from an independent third party. Participants are randomly presented one of the four experimental conditions: (1) more comprehensive cybersecurity risk management examination and no cybersecurity incident, (2) less comprehensive vulnerability and penetration test and no cybersecurity incident (3) more comprehensive cybersecurity risk management examination and cybersecurity incident precedes assurance, and (4) less comprehensive vulnerability and penetration test and cybersecurity incident precedes assurance.

Participants in the cybersecurity incident precedes assurance conditions are presented a management disclosure explaining that management has detected a cybersecurity incident compromising sensitive customer data and has obtained cybersecurity assurance services in response to the cybersecurity incident. Participants in the no cybersecurity incident conditions are not informed of a cybersecurity incident.

Participants in the more comprehensive conditions are provided a management disclosure explaining that management has engaged one of the world’s leading audit, tax, and advisory professional services firms to conduct a cybersecurity risk management program examination. The description of the high assurance service is adapted from an illustrative cybersecurity risk management examination report provided by the AICPA (AICPA 2017b). Comprehensive cybersecurity risk management examinations include all components of a cybersecurity risk management program such as the nature of business operations and information at risk, cybersecurity risk management program objectives, risk assessments, governance structure,
communications, monitoring, and control processes (AICPA 2017b). Alternatively, participants in the less comprehensive vulnerability and penetration test conditions are provided a management disclosure explaining that management engaged one of the world’s leading audit, tax, and advisory professional services firms to conduct an automated vulnerability and penetration test. Less comprehensive vulnerability and penetration tests include only one control within a cybersecurity risk management program (AICPA 2017b). Although vulnerability and penetration tests are offered by many alternative providers (Kuranda 2017), the description of the less comprehensive cybersecurity assurance service is adapted from a cybersecurity risk service currently offered by one of the big four audit, tax, and advisory professional services firms (e.g., Deloitte 2018b). The adaptation of the service used in the experiment focuses on aspects of the service that reflect a less comprehensive assurance service. In addition, examples of recent cybersecurity disclosures made by a leading provider of credit services in the U.S. (Equifax 2017) and a leading provider of health benefits in the U.S. (Anthem 2015) also contribute to the wording of the cybersecurity disclosures used in the experiment.

Participants are then asked to provide their willingness to invest. Next, participants provide their perceptions of cybersecurity assurance services quality and perceptions of management credibility. Finally, participants answer manipulation check and demographic questions.

3.3.3 Dependent Variable

Willingness to Invest. Drawing on prior research (e.g., Elliott, Rennekamp, and White 2015; Tang and Venkataraman 2018), I measure investors’ willingness to invest based on the average of investment attractiveness and investment likelihood. To measure investment attractiveness, I ask participants how attractive an investment in Cost Saver is on a 7-point Likert
scale anchored on 1 (very unattractive) and 7 (very attractive). To measure investment likelihood, participants are asked to assume that they are given $10,000 to invest in the department store retail industry and to indicate the likelihood that they will invest in Cost Saver relative to its peers in the department store retail industry on a 7-point Likert scale anchored on 1 (more likely to invest in peers) and 7 (more likely to invest in Cost Saver).

3.3.4 Other Measured Variables

Perceptions of Cybersecurity Assurance Services Quality. As noted by the SEC, “Cybersecurity efforts must include, in addition to assessment, prevention and mitigation, resilience and recovery” (SEC 2017d, 1). SEC Chairman Clayton further states “we also must recognize…that there will be intrusions, and that a key component of cyber risk management is resilience and recovery” (SEC 2017a, 1). Given the importance of both prevention and recovery in cybersecurity risk management, I measure investors’ perceptions of cybersecurity assurance services quality by asking participants to rate the quality of the cybersecurity assurance service (cybersecurity risk management examination or vulnerability and penetration test) in assessing Cost Saver's ability to (a) prevent future cybersecurity incidents and (b) recover from future cybersecurity incidents that are not prevented. I measure responses on 7-point Likert scales anchored on 1 (very low quality) and 7 (very high quality). I combine the two measures for hypothesis testing and examine the individual measures in additional analyses.

Perceptions of Management Credibility. Mercer’s (2004) disclosure credibility framework suggests that investors’ perceptions of management credibility, external assurance, and contextual factors together effect investors’ valuation judgments. Although I do not manipulate management credibility directly in this study, it is possible that management’s choice to acquire a more comprehensive external assurance service will influence investors’ perceptions
of management credibility (Pflugrath et al. 2011), consistent with source credibility theory (Birnbaum and Stegner 1979) and the importance of the credibility of a message’s source. That is, management’s choice to acquire a more comprehensive cybersecurity assurance service may signal to investors that management is confident in the organization’s cybersecurity risk management program and that management believes that cybersecurity risk management is important to the overall business strategy thereby increasing investors’ perceptions of management credibility. If this signal indeed leads to higher perceptions of management credibility, higher perceptions of management credibility will impact investors’ valuation judgments (Mercer 2004).

Given the uncertainty of how investors will interpret management’s choice to acquire a more comprehensive cybersecurity assurance service, I measure perceptions of management credibility for additional analyses. Specifically, I measure perceptions of the competence of management related to actions taken to manage and reduce cybersecurity risk on a 7-point Likert scale, anchored on 1 (very incompetent) and 7 (very competent) and perceptions of trustworthiness of management related to actions taken to manage and reduce cybersecurity risk on a 7-point Likert scale, anchored on 1 (very untrustworthy) and 7 (very trustworthy). Consistent with prior research (e.g., Koonce and Lipe 2010; Rennekamp 2012), I combine these two measures into a single measure of perceptions of management credibility. I then investigate whether perceptions of management credibility mediate the relation between perceptions of cybersecurity assurance services quality and willingness to invest.
2.11 Results

3.4.1 Manipulation Checks

In order to incentivize effort and attention and following the recommendation in Buchheit et al. (2018), participants are informed that they would be compensated for satisfactory participation as well as an extra bonus if they answer all comprehension and manipulation check questions correctly. Out of a total of 465 complete responses, 320 participants answer both manipulation check questions correctly. The results reported in the paper are based on analyses that include all participants, but results are qualitatively similar when participants failing one or more manipulation check questions are excluded from the analyses.

3.4.2 Descriptive Statistics

Table 3.1 provides descriptive statistics. When no incident is reported, the mean (std dev.) willingness to invest in the more comprehensive assurance condition is 5.55 (0.91) compared to 5.27 (0.95) in the less comprehensive assurance condition. These means appear to provide support for H1 that predicts that when no cybersecurity incident is reported, investors are more willing to invest in the presence of more compared to less comprehensive cybersecurity assurance services. When an incident is reported, the mean (std dev.) willingness to invest in the more comprehensive condition is 4.57 (1.30) compared to 4.09 (1.37) in the less comprehensive condition. This difference, i.e., 0.48, appears to be larger than the difference in the no incident condition, i.e., 0.28, which provides preliminary support for H2. The descriptive statistics also indicate that perceptions of cybersecurity assurance services quality are higher in the more comprehensive conditions (mean=5.48 and 5.16, S.D.=0.87 and 0.89) than in the less comprehensive conditions (mean=4.78 and 4.46, S.D.=1.11 and 1.12). These results provide
initial support for H3a and H3b, which state that the relation between the type of cybersecurity assurance service and willingness to invest will be mediated by perceptions of cybersecurity assurance services quality both in the absence and presence of a prior cybersecurity incident.

3.4.3 Tests of Hypotheses

Table 3.2 shows the results from analysis of variance (ANOVA) that is used to test H1 and H2. In support of H1, the planned comparison reported in Table 3.2 Panel B shows a significantly higher mean willingness to invest in the more comprehensive condition compared to the less comprehensive condition when no cybersecurity incident is reported (p=0.033). Table 3.2 Panel B also shows significantly higher mean willingness to invest in the more comprehensive condition compared to the less comprehensive condition when a cybersecurity incident is reported (p=0.002). These results suggest that a more comprehensive cybersecurity assurance service results in a greater willingness to invest both when there is and when there is not a cybersecurity incident reported prior to the assurance service.

As noted earlier and predicted in H2, the mean willingness to invest differences between the more and less comprehensive conditions reported in Table 3.2 Panel B appear to be higher when an incident is present (0.48) than when it is absent (0.28). However, as reported in Table 3.2 Panel A, the interaction effect is insignificant (p=0.167) and H2 is not supported. This unexpected result may be due to nonprofessional investors’ already heightened awareness of cybersecurity risk even in the absence of a prior incident. Highly publicized incidents such as Equifax, Target, and Yahoo, are increasingly prevalent (SEC 2018b). Nonprofessional investors’ expectations are perhaps similar to regulators with respect to no organization “is immune from cyberattack” (SEC 2018b, 1) and “…there will be intrusions” (SEC 2017a, 1).
H3a and H3b predict that perceptions of cybersecurity assurance services quality will mediate the relation between the type of cybersecurity assurance service and willingness to invest both in the absence of a cybersecurity incident and when a cybersecurity incident precedes assurance. Given the insignificant interaction effect and for ease of exposition, I exclude the interaction effect in the primary test of H3 mediation analyses and thereby do not test H3a and H3b separately. For completeness, after reporting these results I also provide the results from an analysis of conditional indirect effects of type of cybersecurity assurance service on willingness to invest when the mediation analysis includes the interaction effect, which allows for independent tests of H3a and H3b. All mediation analyses are performed using PROCESS (Hayes 2018).

Figure 3.1 and Table 3.3 Panel A show mediation analysis results from a model that includes the two manipulated variables as independent variables, perceptions of cybersecurity assurance services quality as a mediating variable, and willingness to invest as the dependent variable. The results in Figure 3.1 appear to support H3 overall by indicating significant and positive relations between the type of assurance and perceptions of cybersecurity assurance services quality (p<0.001) and between perceptions of cybersecurity assurance services quality and willingness to invest (p<0.001). The results in Table 3.3 Panel A provide more formal support for H3 overall by testing the indirect effect (the mediation effect). More specifically, based on a 95 percent confidence level and 5,000 bootstrap samples (used for all confidence intervals reported), the confidence interval for the indirect effect of the type of assurance on willingness to invest through perceptions of cybersecurity assurance services quality (effect size=0.21) is entirely above zero (0.09 to 0.34). Thus, as predicted by H3 overall, the relation
between type of assurance and willingness to invest is mediated by perceptions of cybersecurity assurance services quality.

An analysis of conditional indirect effects provides more specific support for both H3a and H3b. The conditional indirect effects are based on a model with the type of assurance as the independent variable, cybersecurity incident as a moderating variable, perceptions of cybersecurity assurance services quality as a mediator, and willingness to invest as the dependent variable. The results in Table 3.4 show significant conditional indirect effects for the type to quality to willingness path both when a cybersecurity incident is absent (confidence interval from 0.06 to 0.37) and when a cybersecurity incident is present (confidence interval from 0.01 to 0.41). Further, as expected given the insignificant interaction effect in the ANOVA model, the difference between the two indirect effects is not significant (confidence interval from -0.25 to 0.24).

3.4.4 Additional Analyses

Perceptions of Management Credibility Mediation Analysis. To examine whether perceptions of management credibility mediate the relation between perceptions of cybersecurity assurance services quality and willingness to invest, I examine a serial mediation model with perceptions of cybersecurity assurance services quality and perceptions of management credibility as the mediators between type of assurance and willingness to invest. Figure 3.2 presents the results for the individual paths in this mediation model and Table 3.3 Panel B provides the results for the indirect effects.

The path coefficients in Figure 3.2 are similar to those reported in Figure 3.1 except for the direct effect of perceptions of cybersecurity assurance services quality on willingness to invest, which is 0.66 (p<0.001) in Figure 3.1 and 0.18 (p=0.004) in Figure 3.2. The apparent
decrease in this direct effect is due to the addition of perceptions of management credibility as a mediating variable between perceptions of cybersecurity assurance services quality and willingness to invest. Further, the path between perceptions of cybersecurity assurance services quality and perceptions of management credibility is positive and significant (coef=0.87; p<0.001). The subsequent path between perceptions of management credibility and willingness to invest is also positive and significant (coef=0.57; p<0.001). These two positive effects suggest that perceptions of management credibility acts as a significant mediator between perceptions of cybersecurity assurance services quality and willingness to invest. More formal support for this conjecture is provided by the significant results for the type to quality to credibility to willingness path indirect effect reported in Table 3.3 Panel B. More specifically, the confidence interval for this indirect effect (effect size=0.16) is entirely above zero (0.06 to 0.26).

Prevention versus Recovery Mediation Analysis. Given the importance of both prevention and recovery in cybersecurity risk management, I perform a mediation analyses that replaces the perceptions of cybersecurity assurance services quality mediating variable in Figure 3.1 with two parallel mediators representing the two dimensions of cybersecurity assurance services quality (see Figure 3.3). The two dimensions measure perceptions of the quality of the cybersecurity assurance service in assessing Cost Saver's ability to (a) prevent future cybersecurity incidents and (b) recover from future cybersecurity incidents that are not prevented.

Figure 3.3 and Table 3.3 Panel C present the parallel mediation model results. Figure 3.3 shows that the type of assurance has a positive and significant effect on recover (coef=0.54; p<0.001) and an insignificant effect on prevent (coef=0.10; p=0.329). Table 3.3 Panel C
showing results for the indirect effects with *recover* and *prevent* as the mediators between type of assurance and willingness to invest provide similar results. The *type to recover to willingness* path indirect effect is significant (confidence interval from 0.08 to 0.25), but the *type to prevent to willingness* path indirect effect is not significant (confidence interval from -0.04 to 0.12). Additionally, a comparison of the two indirect effects indicates that the *recover* indirect effect is significantly more positive than the *prevent* indirect effect (confidence interval from 0.01 to 0.22). These results suggest that the more comprehensive conditions result in higher perceptions of cybersecurity assurance services quality primarily because of the perception that the company is more prepared to recover from future cybersecurity incidents that are not prevented.

### 2.12 Conclusion

In response to increasing cybersecurity risks, the AICPA recently released a cybersecurity risk management examination service designed to provide assurance about organizations’ cybersecurity risk management programs (AICPA 2017a). Considering the voluntary and non-standardized nature of the current cybersecurity risk management assurance services market (AICPA 2017a; Kuranda 2017) and the limited success of a previous AICPA IT-related voluntary assurance reporting initiative called WebTrust (Mauldin and Arunachalam 2002; Gendron and Barrett 2004), it is important to understand how the new comprehensive AICPA cybersecurity service would be perceived by stakeholders. I conduct an experiment to investigate how nonprofessional investors perceive and react to management disclosures related to alternative types of external cybersecurity assurance. I focus specifically on nonprofessional investors because the SEC is concerned about the grave cybersecurity threats facing the investing public and the need for more robust cybersecurity disclosures (SEC 2017b, 2018a).
I find that investors are more willing to invest when management disclosures describe a more compared to less comprehensive type of cybersecurity assurance service. This result is significant both in the absence of a reported cybersecurity incident and when a cybersecurity incident precedes cybersecurity assurance. I also find that investors’ perceptions of cybersecurity assurance services quality mediate the relation between type of cybersecurity assurance service and willingness to invest. Additional analyses suggest that a more comprehensive assurance service results in higher perceptions of cybersecurity assurance services quality because of the perception that the company is more prepared to recover from future cybersecurity incidents that are not prevented. The results also show that management’s choice to acquire a more comprehensive external cybersecurity assurance service has a positive effect on investor perceptions of management credibility, which in turn has a positive effect on willingness to invest.

This study makes three contributions to research and practice. First, this study contributes to the growing literature related to cybersecurity assurance disclosures. Using an experimental method, I am able to examine effects of the AICPA’s new cybersecurity risk management examination service in comparison to competing external assurance services and answer the AICPA’s call for research on how users react to cybersecurity assurance reporting (AAA 2017a, 2017b). I also shed light on investors’ perceptions of vital aspects of cybersecurity risk management assurance in terms of an organization’s ability to not only prevent future cybersecurity incidents, but also to recover from future incidents that are not prevented – an important finding as cybersecurity incidents are inevitable and a key component of cybersecurity risk management is recovery (SEC 2017a, 2017d).
Second, I contribute to the voluntary assurance disclosure literature by examining investors’ reactions to managements’ disclosures of alternative types of voluntary external cybersecurity assurance service and show that the comprehensiveness of the voluntary assurance service voluntarily disclosed by management affects users’ judgments and decisions. I also find that management’s choice to acquire a more comprehensive cybersecurity assurance service has a positive effect on investor perceptions of management credibility, which in turn has a positive effect on willingness to invest. Management’s choice may signal to investors that management is confident in the organization’s cybersecurity risk management program and that management believes that cybersecurity risk management is important to the overall business strategy.

Third, this study makes an important contribution to practice. The new cybersecurity risk management examination service shares many features with the AICPA’s previous WebTrust service that did not fare well in the marketplace. Yet, providing preliminary evidence that the AICPA’s new SOC for Cybersecurity service may garner greater market acceptability, my results suggest that nonprofessional investors are sensitive to the type of cybersecurity assurance service provided, and companies can benefit from investing in more comprehensive cybersecurity risk management assurance services such as the AICPA’s SOC for Cybersecurity. This is an important finding given that cybersecurity has become a top concern for public companies and their boards who are looking to CPA firms to increasingly report on cybersecurity program effectiveness (AICPA 2018; Deloitte 2018a; EY 2018; AAA 2019).

These findings should be interpreted in light of certain limitations that can also provide future research opportunities. First, although the new cybersecurity guidance from regulators (SEC 2018a; NIST 2018) is in the process of being widely publicized to nonprofessional investors in the popular press, it is possible that the observed results will not generalize to less
informed investors. Future studies could also examine whether professional investors react differently than nonprofessional investors to alternative voluntary cybersecurity assurance service disclosures. Second, the retail industry is held constant to control for industry effects and to make the setting more salient to nonprofessional investors. However, future research could examine whether alternative cybersecurity assurance services affect investors’ perceptions and decisions differently by industry. Third, to explore potential differences between the AICPA’s new cybersecurity risk management examination service and competing assurance services the service provider is held constant in the manipulations. By instead holding the cybersecurity assurance service constant, future research could examine the effects of the service provider on investor perceptions and decisions. Such research could also be designed to examine investors’ perceptions of CPAs’ expertise in the context of cybersecurity assurance services.
### Table 3.1: Essay 2 Descriptive Statistics – Mean (Standard Deviations)

<table>
<thead>
<tr>
<th>Type of Cybersecurity Assurance Service</th>
<th>Cybersecurity Incident</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No Incident</td>
<td>Incident Precedes Assurance</td>
<td>Row Means</td>
<td></td>
</tr>
<tr>
<td><strong>More Comprehensive</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willingness to Invest</td>
<td>5.55 (0.91)</td>
<td>4.57 (1.30)</td>
<td>5.06 (1.22)</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Assurance Services Quality</td>
<td>5.48 (0.87)</td>
<td>4.78 (1.11)</td>
<td>5.13 (1.06)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>n = 118</td>
<td>n = 117</td>
<td>n = 235</td>
<td></td>
</tr>
<tr>
<td><strong>Less Comprehensive</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willingness to Invest</td>
<td>5.27 (0.95)</td>
<td>4.09 (1.37)</td>
<td>4.69 (1.32)</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Assurance Services Quality</td>
<td>5.16 (0.89)</td>
<td>4.46 (1.12)</td>
<td>4.82 (1.07)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>n = 117</td>
<td>n = 113</td>
<td>n = 230</td>
<td></td>
</tr>
<tr>
<td><strong>Column Means</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Willingness to Invest</td>
<td>5.41 (0.94)</td>
<td>4.34 (1.36)</td>
<td>4.88 (1.28)</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Assurance Services Quality</td>
<td>5.32 (0.9)</td>
<td>4.62 (1.13)</td>
<td>4.98 (1.07)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>n = 235</td>
<td>n = 230</td>
<td>n = 465</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** *Willingness to Invest* includes investment attractiveness and investment likelihood. Participants rate investment attractiveness and investment likelihood on a seven-point scales with endpoints “very unattractive” and “very attractive” and endpoints “very likely to invest in peers” and “very likely to invest in Cost Saver” respectively. *Perceptions of Cybersecurity Assurance Services Quality* includes perceptions of prevent and recover. Participants rate the quality of the assurance service in assessing Cost Saver's ability to (a) prevent future cybersecurity incidents and (b) recover from future cybersecurity incidents that are not prevented on seven-point scales with endpoints “very low quality” and “very high quality.”
Table 3.2: The Effect of Type of Cybersecurity Assurance Service and Cybersecurity Incident on Willingness to Invest

Panel A: Conventional ANOVA

<table>
<thead>
<tr>
<th>Source</th>
<th>df</th>
<th>MS</th>
<th>F-value</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Cybersecurity Assurance Service</td>
<td>1</td>
<td>16.848</td>
<td>12.708</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>Cybersecurity Incident</td>
<td>1</td>
<td>135.959</td>
<td>102.549</td>
<td>&lt; 0.001</td>
</tr>
<tr>
<td>Assurance X Incident (H2)</td>
<td>1</td>
<td>1.243</td>
<td>0.937</td>
<td>0.167</td>
</tr>
<tr>
<td>Error</td>
<td>461</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Panel B: Planned Comparison

<table>
<thead>
<tr>
<th>Relation</th>
<th>Mean Difference</th>
<th>F-value</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>More &gt; Less Comprehensive for No Incident (H1)</td>
<td>0.277</td>
<td>3.408</td>
<td>0.033</td>
</tr>
<tr>
<td>More &gt; Less Comprehensive for Incident</td>
<td>0.484</td>
<td>10.163</td>
<td>0.002</td>
</tr>
</tbody>
</table>

Notes: P-values are reported one-tailed when the path coefficient is in the expected direction, otherwise two-tailed. Cybersecurity Incident is manipulated as no cybersecurity incident or cybersecurity incident precedes cybersecurity assurance. Type of Cybersecurity Assurance Service is manipulated as more or less comprehensive. Willingness to Invest includes investment attractiveness and investment likelihood. Participants rate investment attractiveness and investment likelihood on a seven-point scales with endpoints “very unattractive” and “very attractive” and endpoints “very likely to invest in peers” and “very likely to invest in Cost Saver” respectively.
Table 3.3: Indirect Effects of Type of Cybersecurity Assurance Service on Willingness to Invest

<table>
<thead>
<tr>
<th>Panel A: Cybersecurity Assurance Services Quality Mediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paths&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Type → Quality → Willingness</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Panel B: Perceptions of Management Credibility Mediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paths&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Total</td>
</tr>
<tr>
<td>Type → Quality → Willingness</td>
</tr>
<tr>
<td>Type → Credibility → Willingness</td>
</tr>
<tr>
<td>Type → Quality → Credibility → Willingness</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Panel C: Prevent versus Recover Mediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paths&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>Total</td>
</tr>
<tr>
<td>Type → Prevent → Willingness</td>
</tr>
<tr>
<td>Type → Recover → Willingness</td>
</tr>
<tr>
<td>Indirect effect contrast</td>
</tr>
</tbody>
</table>

<sup>a</sup> Type of Cybersecurity Assurance Service is manipulated as more or less comprehensive. Willingness to Invest includes investment attractiveness and investment likelihood on a seven-point scales with endpoints “very unattractive” and “very attractive” and endpoints “very likely to invest in peers” and “very likely to invest in Cost Saver” respectively. Perceptions of Cybersecurity Assurance Services Quality includes perceptions of prevent and recover. Participants rate the quality of the assurance service in assessing Cost Saver's ability to (a) prevent future cybersecurity incidents and (b) recover from future cybersecurity incidents that are not prevented on seven-point scales with endpoints “very low quality” and “very high quality.” Perceptions of Management Credibility includes perceptions of management competence and trustworthiness. Participants rate management competence and trustworthiness on a seven-point scales with endpoints “very incompetent” and “very competent” and endpoints “very untrustworthy” and “very trustworthy” respectively.

<sup>b</sup> All mediation analyses are performed using PROCESS (Hayes 2018) with 5,000 bootstrap samples and 95% level of confidence.
Table 3.4: Conditional Indirect Effects of Type of Assurance on Willingness to Invest

<table>
<thead>
<tr>
<th>Condition</th>
<th>Paths</th>
<th>Effect</th>
<th>Standard Error</th>
<th>Confidence Interval Limits</th>
<th>Indirect effect contrast</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident = 0</td>
<td>Type → Quality → Willingness</td>
<td>0.21</td>
<td>0.08</td>
<td>0.06, 0.37</td>
<td></td>
</tr>
<tr>
<td>Incident = 1</td>
<td>Type → Quality → Willingness</td>
<td>0.21</td>
<td>0.10</td>
<td>0.01, 0.41</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect effect contrast</td>
<td>0.00</td>
<td>0.12</td>
<td>-0.25, 0.24</td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) Cybersecurity Incident is manipulated as no cybersecurity incident or cybersecurity incident precedes cybersecurity assurance. Type of Cybersecurity Assurance Service is manipulated as more or less comprehensive. Willingness to Invest includes investment attractiveness and investment likelihood. Participants rate investment attractiveness and investment likelihood on a seven-point scales with endpoints “very unattractive” and “very attractive” and endpoints “very likely to invest in peers” and “very likely to invest in Cost Saver” respectively. Perceptions of Cybersecurity Assurance Services Quality includes perceptions of prevent and recover. Participants rate the quality of the assurance service in assessing Cost Saver's ability to (a) prevent future cybersecurity incidents and (b) recover from future cybersecurity incidents that are not prevented on seven-point scales with endpoints “very low quality” and “very high quality.”

\(^b\) All mediation analyses are performed using PROCESS (Hayes 2018) with 5,000 bootstrap samples and 95% level of confidence.

\(^c\) Indirect effects are tested when a cybersecurity incident is absent (Incident = 0) and when a cybersecurity incident precedes cybersecurity assurance (Incident = 1).
2.14 Figures for Essay 2

Figure 3.1: Perceptions of Cybersecurity Assurance Services Quality Mediation Analysis

Notes: Path coefficients and p-values are obtained using PROCESS (Hayes 2018) with 5,000 bootstrap samples and 95% level of confidence.

Cybersecurity Incident is manipulated as no cybersecurity incident or cybersecurity incident precedes cybersecurity assurance. Type of cybersecurity assurance service is manipulated as more or less comprehensive. Willingness to Invest includes investment attractiveness and investment likelihood. Participants rate investment attractiveness and investment likelihood on a seven-point scales with endpoints “very unattractive” and “very attractive” and endpoints “very likely to invest in peers” and “very likely to invest in Cost Saver” respectively. Perceptions of Cybersecurity Assurance Services Quality includes perceptions of prevent and recover. Participants rate the quality of the assurance service in assessing Cost Saver's ability to (a) prevent future cybersecurity incidents and (b) recover from future cybersecurity incidents that are not prevented on seven-point scales with endpoints “very low quality” and “very high quality.”
Figure 3.2: Perceptions of Management Credibility Mediation Analysis

Notes: Path coefficients and p-values are obtained using PROCESS (Hayes 2018) with 5,000 bootstrap samples and 95% level of confidence. 

*Cybersecurity Incident* is manipulated as no cybersecurity incident or cybersecurity incident precedes cybersecurity assurance. *Type of cybersecurity assurance service* is manipulated as more or less comprehensive. *Willingness to Invest* includes investment attractiveness and investment likelihood. Participants rate investment attractiveness and investment likelihood on a seven-point scales with endpoints “very unattractive” and “very attractive” and endpoints “very likely to invest in peers” and “very likely to invest in Cost Saver” respectively. *Perceptions of Cybersecurity Assurance Services Quality* includes perceptions of prevent and recover. Participants rate the quality of the assurance service in assessing Cost Saver's ability to (a) prevent future cybersecurity incidents and (b) recover from future cybersecurity incidents that are not prevented on seven-point scales with endpoints “very low quality” and “very high quality.” *Perceptions of Management Credibility* includes perceptions of management competence and trustworthiness. Participants rate management competence and trustworthiness on a seven-point scales with endpoints “very incompetent” and “very competent” and endpoints “very untrustworthy” and “very trustworthy” respectively.
Figure 3.3: Perceptions of Cybersecurity Assurance Services Quality: Prevent versus Recover Mediation Analysis

Notes: Path coefficients and p-values are obtained using PROCESS (Hayes 2018) with 5,000 bootstrap samples and 95% level of confidence. Cybersecurity Incident is manipulated as no cybersecurity incident or cybersecurity incident precedes cybersecurity assurance. Type of cybersecurity assurance service is manipulated as more or less comprehensive. Willingness to Invest includes investment attractiveness and investment likelihood. Participants rate investment attractiveness and investment likelihood on a seven-point scales with endpoints “very unattractive” and “very attractive” and endpoints “very likely to invest in peers” and “very likely to invest in Cost Saver” respectively. Perceptions of Cybersecurity Assurance Services Quality includes perceptions of prevent and recover. Participants rate the quality of the assurance service in assessing Cost Saver's ability to (a) prevent future cybersecurity incidents and (b) recover from future cybersecurity incidents that are not prevented on seven-point scales with endpoints “very low quality” and “very high quality.”
Chapter 4. Dissertation Conclusion

The first essay, *The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions*, examines the effect of voluntary disclosures of joint or separate provisioning of cybersecurity risk management examinations on investor perceptions and decisions, and whether these effects differ when a subsequent cybersecurity incident occurs. Interestingly, I find that the negative signal of a subsequent cybersecurity incident reverses investors’ positive perceptions of auditor competence and increases investors’ sensitivity to potential independence impairments when the cybersecurity risk management examination is jointly provisioned, leading to lower perceptions of audit quality. I also find that investors are less willing to invest when the cybersecurity risk management examination is jointly compared to separately provisioned. My results provide important insights to regulators and standard setters who have raised concerns regarding the importance of addressing cybersecurity risk in the integrated internal control over financial reporting and financial statements audits and the potential for independence impairments from increased auditor performed non-audit services such as the cybersecurity examination service. My study also contributes to the non-audit services literature not only by examining a unique and emerging non-audit service not previously examined, but also by showing that non-audit services are perceived differently depending on whether a negative signal of non-audit service quality is present.

Essay 2, *The Impact of the Type of Cybersecurity Assurance Service and Cybersecurity Incidents on Investor Perceptions and Decisions* examines the effect of the type of cybersecurity
assurance service on investor perceptions and decisions and whether these effects differ when a prior cybersecurity incident is reported. I find that investors are more willing to invest and have higher perceptions of management credibility when voluntary disclosures include a cybersecurity risk management examination compared to a less comprehensive cybersecurity assurance service. These findings are important because public company boards are increasingly looking to audit firms to provide cybersecurity assurance services. I also find that investors perceive cybersecurity risk management examinations to provide higher assurance quality regarding an organization’s ability not only to prevent future cybersecurity incidents, but also to recover from those that are not prevented - a key risk management issue raised by regulators. My study also contributes to the voluntary assurance disclosure literature by examining investor reactions to management disclosures of alternative types of voluntary external cybersecurity assurance service, beyond a comparison of the absence or presence of external assurance reports provided by CPAs previously examined in other non-financial voluntary assurance settings. I also find that management’s choice to acquire a more comprehensive cybersecurity assurance service has a positive effect on investors’ perceptions of management credibility, which in turn has a positive effect on investors’ willingness to invest.

Both essays contribute to the growing literature related to cybersecurity risks. Most of this work has been archival in nature and as such, has not been able to examine the effects of the AICPA’s recently adopted cybersecurity risk management examination reporting. Using an experimental method, I am able to examine important implications of voluntary cybersecurity risk management examination reporting and present several opportunities for future research. First, future research could examine whether professional investors react differently than nonprofessional investors to cybersecurity risk management examination and cybersecurity
incident disclosures. Second, I hold the retail industry constant in both essays to control for industry effects and make the setting more salient to the participants. Future research could examine whether cybersecurity risk management examination and cybersecurity incident disclosures impact investors’ perceptions and decisions differently by industry. Third, the cybersecurity assurance service providers examined in both essays are the large audit firms. Future research could examine investor perceptions of CPAs’ expertise in the context of cybersecurity risk management examinations. Fourth, future research could examine variables in addition to perceptions of competence, independence, and audit quality that provide additional insights into investors’ judgment and decision making in the context of joint provisioning of cybersecurity non-audit services. Fifth, although archival data on the level of fees associated with cybersecurity risk management examination non-audit services are not yet available, the experimental method could be used in future research to examine the impact of the level of cybersecurity examination fees on investor perceptions and decisions. Finally, future research could examine the impact of alternative cybersecurity incidents, i.e., type of incident, type of information or other asset compromised, length, timing, and severity of the security event, etc., on investor perceptions and decisions in the context of voluntary cybersecurity risk management examination disclosures.
Chapter 5. References

5.1 References for Essay 1


_____. 2017b. Cybersecurity Risk Management Program Examination Engagements; Panelists: Erin Mackler, AICPA; Catherine Nance, Center for Audit Quality; Chris Halterman, EY and AICPA’s ASEC Cybersecurity Working Group. AAA Auditing Section Midyear, January 14, 2017, Orlando, FL.

_____. 2019. The PCAOB’s New Strategic Plan: What Will It Mean for the Auditing Profession? Panelists: Francis “Abe” Dymond, PCAOB Chief of Staff; Trent Gazzaway, Grant Thornton LLP; and Joe Ucuzoglu, Deloitte & Touche LLP. AAA Auditing Section Midyear, January 18, 2019, Nashville, TN.


_____. 2017a. *SOC for Cybersecurity a Backgrounder*. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadeddocuments/soc-for-cybersecurity-backgrounder.pdf


McKenna, Francine. 2018. *Unit of Equifax’s auditor EY certified the information security that was later breached*. MarketWatch: December 18. Available at: https://www.marketwatch.com/story/unit-of-equifaxes-auditor-ey-certified-the-information-security-that-was-later-breached-2018-12-20


5.2 References for Essay 2


_____ 2019. The PCAOB’s New Strategic Plan: What Will It Mean for the Auditing Profession? Moderator: Cynthia Fornelli, Center for Audit Quality. Panelists: Francis “Abe” Dymond, PCAOB Chief of Staff; Trent Gazzaway, Grant Thornton LLP; and Joe Uezoglu, Deloitte & Touche LLP. AAA Auditing Section Midyear, January 18, 2019, Nashville, TN.


Chapter 6. Appendices
Appendix A: Experimental Instrument for Essay 1

Instructions: Please assume the role of a potential investor and carefully consider all the information in the following case before answering the questions that follow.

Background and Initial Valuation

Background
Cost Saver Corporation operates a national chain of discount department stores. Cost Saver has over 11,800 stores nationwide and grew rapidly in the late 1990s and early 2000s by adding additional stores. Similar to many other retailers, Cost Saver is making significant investments in ecommerce and in 2017 online sales accounted for 16.4% of total sales. To drive a greater proportion of their sales through their ecommerce website, Cost Saver provides promotions and makes it easy for in-store customers to create online user profiles by automatically (after consent from the customer) storing their personal and payment information.

Cost Saver Stock Information
Cost Saver released its 2017 fiscal year financial statements on February 15, 2018. Cost Saver’s 2017 sales increased by 6.5 percent compared to analyst expectations of 6.1 percent and earnings increased by 8.1 percent compared to analyst expectations of 6.3 percent. Analysts increased the stock price target from $56 the day before the results were released to $70 the day after the results were released. Cost Saver’s stock closing price was $50 the day before the financial statement were released.

Audit Engagement
Big 4 Firm A has been Cost Saver’s auditor for the past six years. Big 4 Firm A is one of the four largest global accounting firms offering audit, assurance, consulting, and tax services. The local office that performs the Cost Saver audit has extensive experience auditing companies in the retail industry, but Cost Saver is one of the local office’s largest and most complex clients, especially in terms of internal controls. Cost Saver’s move towards increasing reliance on ecommerce has further increased the importance and complexity of the internal controls over financial reporting evaluation on the Cost Saver audit. The audit of Cost Saver has, however, been fairly eventless and Cost Saver received a clean financial statement audit opinion and clean internal controls over financial reporting opinion just as it has in each of the past six years.
Were Cost Saver’s earnings better or worse than analyst expectations?

- Better (1)
- Worse (2)

Has Cost Saver’s move towards increasing reliance on ecommerce further increased the importance and complexity of the internal controls evaluation on the Cost Saver audit?

- Yes (1)
- No (2)
<table>
<thead>
<tr>
<th>In your opinion, how attractive of an investment is Cost Saver? (1)</th>
<th>Very Unattractive (1)</th>
<th>Unattractive (2)</th>
<th>Somewhat Unattractive (3)</th>
<th>Neither Attractive nor Unattractive (4)</th>
<th>Somewhat Attractive (5)</th>
<th>Attractive (6)</th>
<th>Very Attractive (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Very Unlikely (1)</td>
<td>Unlikely (2)</td>
<td>Somewhat Unlikely (3)</td>
<td>Neither Likely nor Unlikely (4)</td>
<td>Somewhat Likely (5)</td>
<td>Likely (6)</td>
<td>Very Likely (7)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------</td>
<td>--------------</td>
<td>-----------------------</td>
<td>---------------------------------</td>
<td>--------------------</td>
<td>------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Assuming you were given $10,000 to invest in the department store retail industry, how likely are you to invest a portion of this amount in the stock of Cost Saver? (1)</td>
<td>☐ ☐ ☐ ☐ ☐ ☐ ☐</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


**Cybersecurity Examination**

Cost Saver makes significant investments in cybersecurity to support its strategy to grow online sales. In response to increasing public concern about cybersecurity threats, especially in the wake of highly publicized attacks at Target and Yahoo, Cost Saver decided to make a voluntary disclosure about these investments and its cybersecurity risk management program. In the disclosure, Cost Saver’s management asserted that Cost Saver maintained effective controls over cybersecurity risk management as described by the criteria established by the AICPA.

Further, Cost Saver decided to hire an independent third party to perform an annual examination of the effectiveness of the controls within the cybersecurity risk management program. Cost Saver decided to hire Big 4 Firm A, the same firm that currently performs the audit of financial statements and related internal controls, to conduct the cybersecurity examination.

Big 4 Firm A performed the cybersecurity examination during the same time period that the financial statement and related internal controls audit work was performed. The cybersecurity assessment resulted in a clean opinion. That is, Big 4 Firm A concluded that management’s assertion that the company maintained, in all material respects, effective internal controls over cybersecurity risk management as of December 31, 2017, based on criteria established by the AICPA was fairly stated. The report was issued on February 15, 2018, the same day that the financial statements were released.

As of March 8, 2018, three weeks after Cost Saver released its financial statements and cybersecurity examination disclosure and related clean audit opinions, Cost Saver has not detected any cybersecurity incidents (breaches).
Cybersecurity Examination
Cost Saver makes significant investments in cybersecurity to support its strategy to grow online sales. In response to increasing public concern about cybersecurity threats, especially in the wake of highly publicized attacks at Target and Yahoo, Cost Saver decided to make a voluntary disclosure about these investments and its cybersecurity risk management program. In the disclosure, Cost Saver's management asserted that Cost Saver maintained effective controls over cybersecurity risk management as described by the criteria established by the AICPA.

Further, Cost Saver decided to hire an independent third party to perform an annual examination of the effectiveness of the controls within the cybersecurity risk management program. Cost Saver decided to hire Big 4 Firm B, a different firm than the current financial statement and related internal controls auditors, to conduct the cybersecurity examination.

Big 4 Firm B performed the cybersecurity examination during the same time period that the financial statement and related internal controls audit work was performed. The cybersecurity assessment resulted in a clean opinion. That is, Big 4 Firm B concluded that management's assertion that the company maintained, in all material respects, effective internal controls over cybersecurity risk management as of December 31, 2017, based on criteria established by the AICPA was fairly stated. The report was issued on February 15, 2018, the same day that the financial statements were released.

As of March 8, 2018, three weeks after Cost Saver released its financial statements and cybersecurity examination disclosure and related clean audit opinions, Cost Saver has not detected any cybersecurity incidents (breaches).
Cost Saver makes significant investments in cybersecurity to support its strategy to grow online sales. In response to increasing public concern about cybersecurity threats, especially in the wake of highly publicized attacks at Target and Yahoo, Cost Saver decided to make a voluntary disclosure about these investments and its cybersecurity risk management program. In the disclosure, Cost Saver’s management asserted that Cost Saver maintained effective controls over cybersecurity risk management as described by the criteria established by the AICPA.

Further, Cost Saver decided to hire an independent third party to perform an annual examination of the effectiveness of the controls within the cybersecurity risk management program. Cost Saver decided to hire Big 4 Firm A, the same firm that currently performs the audit of financial statements and related internal controls, to conduct the cybersecurity examination.

Big 4 Firm A performed the cybersecurity examination during the same time period that the financial statement and related internal controls audit work was performed. The cybersecurity assessment resulted in a clean opinion. That is, Big 4 Firm A concluded that management’s assertion that the company maintained, in all material respects, effective internal controls over cybersecurity risk management as of December 31, 2017, based on criteria established by the AICPA was fairly stated. The report was issued on February 15, 2018, the same day that the financial statements were released.

On March 8, 2018, three weeks after Cost Saver released its financial statements and cybersecurity examination disclosure and related clean audit opinions, Cost Saver issued the following statement publicly: “We have detected a cybersecurity incident that occurred in the first week of March 2018. The breach allowed criminals to gain access to sensitive customer data, including name, birth dates, home addresses, and credit card numbers, expiration dates and security codes. We believe that up to 20 million customer accounts were impacted.”
Cybersecurity Examination
Cost Saver makes significant investments in cybersecurity to support its strategy to grow online sales. In response to increasing public concern about cybersecurity threats, especially in the wake of highly publicized attacks at Target and Yahoo, Cost Saver decided to make a voluntary disclosure about these investments and its cybersecurity risk management program. In the disclosure, Cost Saver’s management asserted that Cost Saver maintained effective controls over cybersecurity risk management as described by the criteria established by the AICPA.

Further, Cost Saver decided to hire an independent third party to perform an annual examination of the effectiveness of the controls within the cybersecurity risk management program. Cost Saver decided to hire Big 4 Firm B, a different firm than the current financial statement and related internal controls auditors, to conduct the cybersecurity examination.

Big 4 Firm B performed the cybersecurity examination during the same time period that the financial statement and related internal controls audit work was performed. The cybersecurity assessment resulted in a clean opinion. That is, Big 4 Firm B concluded that management’s assertion that the company maintained, in all material respects, effective internal controls over cybersecurity risk management as of December 31, 2017, based on criteria established by the AICPA was fairly stated. The report was issued on February 15, 2018, the same day that the financial statements were released.

On March 8, 2018, three weeks after Cost Saver released its financial statements and cybersecurity examination disclosure and related clean audit opinions, Cost Saver issued the following statement publicly: “We have detected a cybersecurity incident that occurred in the first week of March 2018. The breach allowed criminals to gain access to sensitive customer data, including name, birth dates, home addresses, and credit card numbers, expiration dates and security codes. We believe that up to 20 million customer accounts were impacted.”
You previously indicated that the attractiveness of an investment in Cost Saver was \${PreAttract/ChoiceGroup/SelectedAnswers}. Based on the additional cybersecurity information you have received since then, in your opinion, how attractive of an investment is Cost Saver? (1)
You *previously* indicated that the likelihood that you would invest in Cost Saver was $\{\text{PreInvest/ChoiceGroup/SelectedAnswers}\}$. Based on the **additional cybersecurity information** you have received since then, assuming you *again* were given $10,000 to invest in the department store retail industry, how likely are you to invest a portion of this amount in the stock of Cost Saver? (1)
**Other Measured Variables**

**Competence:** Auditors are competent when they have relevant **knowledge** and the **ability** to use this knowledge in a specific auditing context.

<table>
<thead>
<tr>
<th></th>
<th>Very Unconfident (1)</th>
<th>Unconfident (2)</th>
<th>Somewhat Unconfident (3)</th>
<th>Neither Confident nor Unconfident (4)</th>
<th>Somewhat Confident (5)</th>
<th>Confident (6)</th>
<th>Very Confident (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>How confident are you</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>in Big 4 Firm $e://Field/Firm)'s competence in Cost Saver's cybersecurity examination? (1)</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>How confident are you</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>in Big 4 Firm A's competence in Cost Saver's financial statement and related internal controls audit? (2)</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
**Independence**: Auditors are independent when they act with integrity and objectivity, and without biases, and when they do not give in to pressure from management.

<table>
<thead>
<tr>
<th></th>
<th>Very Unconfident (1)</th>
<th>Unconfident (2)</th>
<th>Somewhat Unconfident (3)</th>
<th>Neither Confident nor Unconfident (4)</th>
<th>Somewhat Confident (5)</th>
<th>Confident (6)</th>
<th>Very Confident (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>How confident are you that Big 4 Firm ${e://Field/Firm}$ acted <strong>independently</strong> when performing Cost Saver’s cybersecurity examination? (1)</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>How confident are you that Big 4 Firm A acted <strong>independently</strong> when performing Cost Saver’s financial statement and related internal controls audit? (2)</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
**Quality:** How confident are you that **sufficient evidence** was obtained and used to support:

<table>
<thead>
<tr>
<th></th>
<th>Very Unconfident (1)</th>
<th>Unconfident (2)</th>
<th>Somewhat Unconfident (3)</th>
<th>Neither Confident nor Unconfident (4)</th>
<th>Somewhat Confident (5)</th>
<th>Confident (6)</th>
<th>Very Confident (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big 4 Firm ${e://Field/Firm}$’s clean opinion that the <strong>cybersecurity controls</strong> are effective and designed as described by Cost Saver? (1)</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Big 4 Firm A’s clean opinion that Cost Saver maintained effective <strong>internal controls</strong> over financial reporting? (2)</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Big 4 Firm A’s clean opinion that the <strong>financial statements</strong> faithfully represent Cost Saver's underlying economics? (3)</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>
Manipulation Checks

Was the audit firm providing the cybersecurity examination the same audit firm providing the financial statement audit and related internal controls audit?

- Yes (1)
- No (2)

Did Cost Saver report a cybersecurity incident (breach)?

- Yes (1)
- No (2)
How many times have you purchased or sold individual stock or mutual funds?
________________________________________________________________

How many accounting or finance courses have you taken?
________________________________________________________________

How many years of work experience do you have?
________________________________________________________________
How many times have you made **online** purchases in the last 3 months?

- Never (1)
- 1-3 times (2)
- 4-6 times (3)
- More than 6 times (4)

How many times have you made **in-store** purchases at a department store in the last 3 months?

- Never (1)
- 1-3 times (2)
- 4-6 times (3)
- More than 6 times (4)
Have you ever been a victim of identity theft or credit card fraud?

- Yes  (1)
- No  (2)

What is your age?

________________________________________________________________

What is your gender?

- Female  (1)
- Male  (2)
- Prefer not to answer  (3)
Appendix B: Experimental Instrument for Essay 2

**Instructions:** Please assume the role of a potential investor and *carefully* consider all the information in the following case before answering the questions that follow.

---

**Regulatory Background**

This section provides you with background information on cybersecurity to inform you of recent guidance from U.S. regulators.

On February 21, 2018, the Securities and Exchange Commission (SEC) issued new guidance for public company cybersecurity disclosures to include descriptions of cybersecurity incidents and actions taken to manage and reduce cybersecurity risk.

One of the leading frameworks for helping organizations manage and reduce cybersecurity risk is the NIST Cybersecurity Framework. The framework includes the following five essential functions:

- **Identify:** Understanding of the business, risk assessment, and governance.
- **Protect:** Processes, controls, and technology to protect information.
- **Detect:** Vulnerability scans and continuous monitoring to detect security events.
- **Respond:** Response planning, analysis, and mitigation.
- **Recover:** Recovery planning, communications, and improvements.
Comprehension Questions

Which of the following functions is **not** included in the NIST Cybersecurity Framework?

- Protect
- Respond
- Recover
- Eliminate

Vulnerability scans is an example of which NIST Cybersecurity Framework function?

- Detect
- Recover
Cost Saver Background

This section provides background information, including the most recent fiscal year-end financial information and e-commerce strategy, about a company that you are considering investing in.

Cost Saver Inc.
(NYSE MKT: CSVR)

Profile Description:
Cost Saver Corporation operates a national chain of discount department stores. The company is listed on NYSE and is included in the S&P 500. Cost Saver has over 11,800 stores nationwide and is headquartered in Denver, Colorado. The company grew rapidly in the late 1990s and early 2000s by adding additional stores. More recently, Cost Saver has been able to continue growing by increasing online sales. Cost Saver’s e-commerce strategy is to both provide low cost and rapid delivery options to customer homes as well as leverage its physical footprint and have customers place orders online and then pick up their purchases at a local Cost Saver store. To drive a greater proportion of its sales through its website, Cost Saver makes it easy for in-store customers to create online user profiles by automatically storing personal and payment information after consent from the customer.

In response to increasing public concern about cybersecurity risk and to support its e-commerce strategy, Cost Saver made the following disclosure: "We have made significant investments in cybersecurity to support our e-commerce growth strategy."

Key Statistics and Ratios:

<table>
<thead>
<tr>
<th></th>
<th>Cost Saver</th>
<th>Industry Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Earnings Per Share (EPS)</td>
<td>$5.33</td>
<td>$4.31</td>
</tr>
<tr>
<td>Price to Earnings (P/E)</td>
<td>13.42</td>
<td>16.58</td>
</tr>
<tr>
<td>Return on Equity (ROE)</td>
<td>25.8%</td>
<td>19.4%</td>
</tr>
<tr>
<td>Sales Growth %</td>
<td>3.0%</td>
<td>2.3%</td>
</tr>
<tr>
<td>Analysts’ Earnings Surprise %</td>
<td>13.1%</td>
<td>4.2%</td>
</tr>
</tbody>
</table>

Source: Yahoo Finance
Comprehension Questions

Were Cost Saver’s earnings better or worse than analyst expectations?

☐ Better

☐ Worse

Has Cost Saver made investments in cybersecurity to support its e-commerce growth strategy?

☐ Yes

☐ No
Condition 1 – More Comprehensive Cybersecurity Examination and No Incident

Subsequent to the most recent fiscal year-end financial information, Cost Saver’s management issued the following statement publicly:

“We engaged one of the world’s leading audit, tax, and advisory professional services firms to conduct a comprehensive cybersecurity risk management program examination including collecting and evaluating evidence regarding controls designed to perform the following five functions:

- protect information and systems from security events, and to
- detect,
- respond to,
- mitigate, and
- recover from security events that are not prevented.

We received a clean attestation opinion supporting:

- our description of our cybersecurity program including business operations and information at risk, cybersecurity objectives, risk assessment, governance structure, communications, monitoring, and control processes, and
- the effectiveness of the controls within our cybersecurity program based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy consistent with the attestation standards established by the AICPA."
Condition 2 – Less Comprehensive Vulnerability and Penetration Test and No Incident

Subsequent to the most recent fiscal year-end financial information, Cost Saver’s management issued the following statement publicly:

“We engaged one of the world’s leading audit, tax, and advisory professional services firms to conduct an automated vulnerability and penetration test and to recommend solutions. The automated vulnerability and penetration test is designed to identify and evaluate gaps in our information technology applications, hardware configurations, and operating systems that are designed to perform the following two functions:

- prevent and
- detect vulnerabilities.

We received a report detailing the results of the automated vulnerability and penetration test including:

- gaps in our information technology applications, hardware configurations, and operating systems, and
- recommended solutions for closing the gaps in our information technology applications, hardware configurations, and operating systems based on our evolving cybersecurity landscape.”
Subsequent to the most recent fiscal year-end financial information, Cost Saver’s management issued the following statement publicly:

“We have detected a cybersecurity incident. The incident allowed criminals to gain access to sensitive customer data, including name, birth dates, home addresses, and credit card numbers, expiration dates and security codes. We believe that up to 20 million customer accounts were impacted. In response, and to position Cost Saver for the future:

We engaged one of the world’s leading audit, tax, and advisory professional services firms to conduct a comprehensive cybersecurity risk management program examination including collecting and evaluating evidence regarding controls designed to perform the following five functions:

- protect information and systems from security events, and to
- detect,
- respond to,
- mitigate, and
- recover from security events that are not prevented.

We received a clean attestation opinion supporting:

- our description of our cybersecurity program including business operations and information at risk, cybersecurity objectives, risk assessment, governance structure, communications, monitoring, and control processes, and

- the effectiveness of the controls within our cybersecurity program based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy consistent with the attestation standards established by the AICPA.”
Subsequent to the most recent fiscal year-end financial information, Cost Saver’s management issued the following statement publicly:

“We have detected a cybersecurity incident. The incident allowed criminals to gain access to sensitive customer data, including names, birth dates, home addresses, and credit card numbers, expiration dates and security codes. We believe that up to 20 million customer accounts were impacted. In response, and to position Cost Saver for the future:

We engaged one of the world’s leading audit, tax, and advisory professional services firms to conduct an automated vulnerability and penetration test and to recommend solutions. The automated vulnerability and penetration test is designed to identify and evaluate gaps in our information technology applications, hardware configurations, and operating systems that are designed to perform the following two functions:

- prevent and
- detect vulnerabilities.

We received a report detailing the results of the automated vulnerability and penetration test including:

- gaps in our information technology applications, hardware configurations, and operating systems, and

- recommended solutions for closing the gaps in our information technology applications, hardware configurations, and operating systems based on our evolving cybersecurity landscape.”
<table>
<thead>
<tr>
<th>Dependent Variable</th>
<th>Very Unattractive (1)</th>
<th>Unattractive (2)</th>
<th>Somewhat Unattractive (3)</th>
<th>Neither Attractive nor Unattractive (4)</th>
<th>Somewhat Attractive (5)</th>
<th>Attractive (6)</th>
<th>Very Attractive (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>In your opinion, how attractive of an investment is Cost Saver?</td>
<td>● ● ○ ○ ● ● ○ ○</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very likely to invest in Peers (1)</td>
<td>Likely to invest in Peers (2)</td>
<td>Somewhat likely to invest in Peers (3)</td>
<td>Indifferent between investing in Peers or Cost Saver (4)</td>
<td>Somewhat likely to invest in Cost Saver (5)</td>
<td>Likely to invest in Cost Saver (6)</td>
<td>Very likely to invest in Cost Saver (7)</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>------------------------------------------</td>
<td>-----------------------------------</td>
<td>--------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Assuming you were given $10,000 to invest in the department store retail industry, what is the likelihood that you will invest in Cost Saver relative to its peers in the department store retail industry?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Measured Variables

How would you rate the quality of the $e://Field/Assurance$ in assessing Cost Saver's ability to:

<table>
<thead>
<tr>
<th></th>
<th>Very Low Quality (1)</th>
<th>Low Quality (2)</th>
<th>Somewhat Low Quality (3)</th>
<th>Neither High nor Low Quality (4)</th>
<th>Somewhat High Quality (5)</th>
<th>High Quality (6)</th>
<th>Very High Quality (7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. prevent future cybersecurity incidents?</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>b. recover from future cybersecurity incidents that are not prevented?</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Very Incompetent (1)</td>
<td>Incompetent (2)</td>
<td>Somewhat Incompetent (3)</td>
<td>Neither Competent nor Incompetent (4)</td>
<td>Somewhat Competent (5)</td>
<td>Competent (6)</td>
<td>Very Competent (7)</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
<td>-------------------------------------</td>
<td>------------------------</td>
<td>--------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>How would you rate the competence of Cost Saver’s management related to actions taken to manage and reduce cybersecurity risk?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very Untrustworthy (1)</td>
<td>Untrustworthy (2)</td>
<td>Somewhat Untrustworthy (3)</td>
<td>Neither Trustworthy nor Untrustworthy (4)</td>
<td>Somewhat Trustworthy (5)</td>
<td>Trustworthy (6)</td>
<td>Very Trustworthy (7)</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>------------------------------------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>How would you rate the <strong>trustworthiness</strong> of Cost Saver's management related to actions taken to manage and reduce cybersecurity risk?</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td></td>
</tr>
</tbody>
</table>
Manipulation Checks

Which cybersecurity service did Cost Saver’s management engage the professional services firm to conduct?

- A vulnerability and penetration test
- A cybersecurity risk management program examination

Did Cost Saver's management report a cybersecurity incident?

- No. Cost Saver's management did not report a cybersecurity incident.
- Yes. The cybersecurity incident impacted over 20 million customer accounts.
Post Experiment Questions

How many times have you purchased or sold individual stocks or mutual funds?
________________________________________________________________

How many accounting or finance courses have you taken?
________________________________________________________________

How many years of work experience do you have?
________________________________________________________________

How many times have you made online purchases in the last 3 months?

○ Never

○ 1-3 times

○ 4-6 times

○ More than 6 times
How many times have you made in-store purchases at a department store in the last 3 months?

- Never
- 1-3 times
- 4-6 times
- More than 6 times

Have you ever been a victim of identity theft or credit card fraud?

- Yes
- No

What is your age?

________________________________________________________________________
Gender What is your gender?

- Female
- Male
- Prefer not to answer
Appendix C: IRB Letter for Essay 1

June 8, 2017

Rebecca Perols
School of Accountancy
Tampa, FL 33612

RE: Exempt Certification
IRB#: Pro00030933
Title: Investor Judgments

Dear Ms. Perols:

On 6/8/2017, the Institutional Review Board (IRB) determined that your research meets criteria for exemption from the federal regulations as outlined by 45CFR46.101(b):

(2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement) survey procedures, interview procedures or observation of public behavior, unless:
(i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and
(ii) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

As the principal investigator for this study, it is your responsibility to ensure that this research is conducted as outlined in your application and consistent with the ethical principles outlined in the Belmont Report and with USF HRPP policies and procedures.

Please note, as per USF HRPP Policy, once the Exempt determination is made, the application is closed in ARC. Any proposed or anticipated changes to the study design that was previously declared exempt from IRB review must be submitted to the IRB as a new study prior to initiation of the change. However, administrative changes, including changes in research personnel, do not warrant an amendment or new application.

Given the determination of exemption, this application is being closed in ARC. This does not limit your ability to conduct your research project.

We appreciate your dedication to the ethical conduct of human subject research at the University of South Florida and your continued commitment to human research protections. If you have any questions regarding this matter, please call 813-974-5638.
Sincerely,

[Signature]

John Schinka, Ph.D., Chairperson
USF Institutional Review Board
Appendix D: IRB Letter for Essay 2

5/1/2018

Rebecca Perols
School of Accountancy
Tampa, FL 33647

RE: Exempt Certification
IRB#: Pro00035149
Title: The Impact of the Level of Cybersecurity External Assurance and Cybersecurity Incidents on Investment Decisions

Dear Ms. Perols:

On 4/30/2018, the Institutional Review Board (IRB) determined that your research meets criteria for exemption from the federal regulations as outlined by 45CFR46.101(b):

(2) Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless:
(i) information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects’ responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

As the principal investigator for this study, it is your responsibility to ensure that this research is conducted as outlined in your application and consistent with the ethical principles outlined in the Belmont Report and with USF HRPP policies and procedures.

Please note, as per USF HRPP Policy, once the Exempt determination is made, the application is closed in ARC. Any proposed or anticipated changes to the study design that was previously declared exempt from IRB review must be submitted to the IRB as a new study prior to initiation of the change. However, administrative changes, including changes in research personnel, do not warrant an amendment or new application.

Given the determination of exemption, this application is being closed in ARC. This does not limit your ability to conduct your research project.

We appreciate your dedication to the ethical conduct of human subject research at the University of South Florida and your continued commitment to human research protections. If you have
any questions regarding this matter, please call 813-974-5638.

Sincerely,

John Schinka, Ph.D., Chairperson
USF Institutional Review Board