Management's Responsibility Acceptance, Locus of Breach, and Investors' Reactions to Internal Control Reports

Hun-Tong Tan
ahttan@ntu.edu.sg
Nanyang Technological University

Yao Yu
yyu@isenberg.umass.edu
University of Massachusetts Amherst

January 8, 2016

We appreciate helpful comments from the editor (Mark Peecher), anonymous reviewers, Wei Chen, Jun Han, Lukas Helikum, Mian-Lian Ho, Terence Ng, Steve Salterio, Premila Shankar, Seet-Koh Tan, Elaine Wang, Zheng Qiao, Wei Qiang, Robert Whited, Feng Yeo,and workshop participants at Nanyang Technological University. We thank Christopher Wolfe for sharing his experimental instrument. We thank Matthew Starliper and Wei Qiang for research assistance.

Management's Responsibility Acceptance, Locus of Breach, and Investors' Reactions to Internal Control Reports

ABSTRACT

We report the results of two experiments that examine the joint effects of two aspects in management's explanations for breaches in the internal control over financial reporting (ICFR): the extent to which management accepts responsibility for the breach, and the locus of the breach (external versus internal). We predict and find that in the presence of an external breach, investors assign less responsibility to management and are more willing to invest in the firm when management accepts more rather than less responsibility (Experiment 1); in contrast, the effect of management's responsibility acceptance reverses in the presence of an internal breach (Experiment 2). We also test our predictions using data hand-collected from 292 ICFR reports. The archival results show that market reactions are less negative when management accepts low (as opposed to high) responsibility for internal breaches.

Keywords: Internal controls over financial reporting, Section 404 of SOX, management explanation, locus of breach, triangle model of responsibility, responsibility assignment.

Data availability: Contact the authors.

I. INTRODUCTION

Section 404 of the Sarbanes-Oxley Act (SOX, U.S. House of Representatives 2002) requires that the management of a public company assesses and discloses the effectiveness of the company's internal control over financial reporting (ICFR). While these disclosures are mandatory, management discussions that generally accompany them are voluntary and their content at management's discretion. In this study, we examine two aspects of management's ICFR discussions: the extent to which management accepts responsibility for a breach of an internal control over financial reporting, and the locus of the breach. We predict and find that these two aspects jointly influence investors' responsibility assignment to management and subsequent assessments of the investment potential of the company.

Examining the effects of the amount of responsibility that management accepts for a breach of an internal control is of interest. Regulators prescribe that management is responsible for maintaining an effective internal control system, and therefore, managers cannot fully deny their responsibility for such breaches. At the same time, standard setters acknowledge that control systems can provide only reasonable, not absolute, assurance for internal control effectiveness (COSO 1992), which enables managers to accept only a small proportion of (but not totally deny) responsibility for internal control lapses, and to utilize this "reasonable assurance" statement as a defense in their internal control reports. [1] Our analysis of actual 10-K disclosures with material internal control weaknesses based on a random sample of 292 ICFR reports between 2009 and 2011 shows that seventy-eight percent of the reports (229 reports) include the reasonable assurance statement (see examples in Appendix A and archival tests in

[1] For instance, according to the COSO framework, "(a)n internal control system, no matter how well conceived and operated, can provide only reasonable—not absolute—assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems" (COSO 1992, 6).

Section V). In the presence of such material internal control weaknesses, whether investors' judgments of the investment attractiveness of the firm are influenced by management's degree of responsibility acceptance is an unanswered question.

We also examine whether this effect is contingent on another aspect of management explanation—the locus of breach (hereafter "breach"); namely, whether the breach that leads to the discovery of an internal control weakness arises from an inside party (e.g., a sales representative hacking into the company's computer system) or an outside party (e.g., an outside hacker; see Appendix A for examples).[2] Examining the effect of breach is particularly important in the context of an information technology security breakdown. Regulators have become increasingly concerned about the repercussions of data breaches and their disclosures. For instance, the Securities and Exchange Commission (2014) requires disclosures of material cyber-security risks and incidents, and has recently investigated companies to assess whether they have adequately handled and disclosed cyber-attacks (Michaels 2014). The manner by which companies disclose such breaches is important because companies are loath to alarm the public and avoid lawsuits, particularly when the breaches involve customers' personal data (Michaels 2014). The issue of breaches by internal versus external parties is particularly important in terms of information technology security—breaches by external parties are more common and well-publicized but damage done as a result of breaches by internal parties can cause more harm (Upton and Creese 2012). How the locus of such breaches interacts with managers' responsibility acceptance in their disclosures to influence investors' judgments is, therefore, an important issue that has not been a subject of investigation.

[2] Among our sample of 292 actual 10-K disclosures, seventy-eight percent of the reports (229 reports) associate their weaknesses with only internal factors, sixteen percent (45 reports) with both internal and external factors, and 1 percent (three reports) with only external factors. Another five percent (15 reports) do not specify the factors related to the weaknesses. See more details in Section V.

We employ the triangle model of responsibility (Schlenker, Britt, Pennington, Murphy, and Doherty 1994) to predict the amount of responsibility that investors assign to management in the event of an internal control failure. According to this model, responsibility assigned to the actor is determined by the strength of three linkages among the prescription, the actor, and the event. The actor is deemed responsible when (1) the prescription (goals, rules and scripts) that is applicable to the event is clearly defined (the prescription-event link), (2) the prescription defines duty or obligation for the actor (the prescription-actor link), and (3) the actor has a control over the event (the actor-event link). In our setting, "prescription" refers to relevant regulations and requirements for the maintenance of a good internal control system, and/or the public's implicit expectations and norms; "actor" refers to firm managers, and "event" refers to the breach. We predict that the strength of the links is affected by locus of breach. The prescription-event link is expected to be stronger for an external breach than for an internal breach. Standard setters and professional bodies (e.g., COSO 1992; Auditing Standards No. 5, PCAOB 2007) make explicit prescriptions about the important role of internal control systems in preventing breaches, but include caveats in the case of *internal* breaches, suggesting that prescription clarity is weaker in the latter. In addition, media coverage of high-profile security attacks, largely by external parties, makes salient the threat of breaches by external party attacks and the need for protection against these attacks. The prescription-actor link is similarly strong for both external and internal breaches because it is widely accepted in litigation and regulations (Section 302 and 404 of SOX) that management is the entity responsible for maintaining an effective control system (U.S. House of Representatives 2002), a responsibility not conditional on the locus of a breach. The actor-event link is stronger in the external breach condition than in the internal breach condition. The reason is that common controls such as access controls and boundary protection of cyber-

assets are targeted more at outsiders and are less effective against insider attacks; hence, internal breaches are less controllable and less preventable than external breaches.

The strength of the links can also be affected by responsibility acceptance (Schlenker, Pontari, and Christopher 2001). For example, when management accepts low responsibility by employing the reasonable assurance argument, this argument weakens the prescription-event link because it suggests that the prescriptions may not apply to certain cases. The reasonable assurance argument also weakens the actor-event link because it implies that some breaches may occur beyond management's control. As a result, low responsibility acceptance can weaken the perceived responsibility of management and lead to more favorable outcomes, compared with high responsibility acceptance. However, accepting low responsibility can be associated with a lack of integrity, reliability, and trustworthiness. We predict that low (as opposed to high) responsibility acceptance leads to more favorable outcomes in an internal breach situation, where the intrusion comes from inside the company and thus is consistent with the message conveyed in the reasonable assurance argument. This consistency attenuates the negative attributes associated with low responsibility acceptance. In contrast, we predict that high responsibility acceptance leads to better outcomes than low responsibility acceptance in an external breach situation, where the reasonable assurance argument is no longer persuasive and the benefits of high responsibility acceptance (e.g., showing management's integrity and willingness to remediate the weakness) become more prominent.

We conduct two experiments to test our predictions. In Experiment 1, we conduct a 2 × 2 between-subjects experiment with responsibility acceptance (high vs. low) and breach (external vs. internal) as independent variables. We manipulate responsibility acceptance by having management accept either a high or low level of responsibility for the breach of control

weakness. We manipulate the breach to be either external (an outsider hacking into the company's computer system) or internal (a sales representative hacking into the company's computer system) to the company. Participants assume the role of general investors evaluating a hypothetical firm's investment attractiveness. They receive the firm's background information and the internal control disclosure, and answer a series of questions including their willingness to invest in the firm and the extent to which they assign responsibility to management for the breach. We find that high responsibility acceptance results in more favorable evaluations and outcomes than low responsibility acceptance with an external breach, consistent with our theoretical predictions. However, the effect of responsibility acceptance is insignificant with an internal breach, inconsistent with our theory.

As a further test of our theory, we conduct Experiment 2 where we strengthen the prescription-event and actor-event links in the internal breach condition. We manipulate link strength (weak vs. strong) and responsibility acceptance (high vs. low) between-subjects, with all conditions set in the internal breach situation. In the strong-link condition, we add a statement warning management that companies need to implement measures to guard against internal breaches. This statement is absent in the weak-link condition, making it equivalent to the original internal breach condition in Experiment 1. The responsibility acceptance variable is manipulated the same way as in Experiment 1. Results are consistent with our predictions. Low responsibility acceptance leads to more favorable evaluations and outcomes than high responsibility acceptance in the strong-link condition, and this effect remains insignificant in the weak-link condition.

Besides the two experiments, we also conduct an archival test with 292 ICFR reports between 2009 and 2011. We code the locus of the factors (internal versus external) related to the internal control weaknesses and the extent to which management accepts responsibility. The

regression results show that, with the majority (78 percent) of the reports mentioning only internal factors, the cumulative market returns over a five-day window surrounding the filing date increase around six to seven percent when management accepts low (as opposed to high) responsibility. This result is consistent with our theory that low responsibility acceptance leads to more favorable outcomes in the situation of internal breaches.

Our results suggest that it is incomplete to assess the efficacy of management explanation type (here, high or low responsibility acceptance) in isolation without considering the effect of the locus of breach (internal or external to the company). Our theory and findings not only provide a useful framework to integrate and interpret related prior studies, but also further refine the theories employed in these studies by explicitly analyzing the effect of locus, a variable that has been ignored in prior studies but impacts their results. For instance, in an auditor-management negotiation setting, Wolfe, Mauldin, and Diaz (2009) examine whether management acknowledgement of the existence of a control deficiency (concession) or denial of its existence (denial) influences auditors' judgments.[3] They conclude that for information technology (IT) control deviations, auditors assess that the deficiency is less significant in the presence of concessions than denials, while for manual control deviations, there is no difference between concessions and denials. Their theoretical argument is that the presence of an irrelevant, non-diagnostic technology element (e.g., the IT element) dilutes perceived management blame, and thus, concessions are more effective than denials in an IT condition. We extend Wolfe et al.

[3] Wolfe et al. (2009) employ a setting of auditor-management negotiation in determining the severity of the internal control deviations. Before reaching an agreement, management has a chance to deny the existence of weaknesses. However, in our setting of internal control over financial reporting, management and the auditors have already reached an agreement on the existence and severity of the weakness. Management cannot deny the existence of the weakness, and can only choose the amount of responsibility that they are willing to accept for this weakness. The "concession" condition in Wolfe et al. (2009) and the "high responsibility acceptance" condition in our paper share the same components—recognizing the existence of the weakness as well as taking a large proportion of responsibility for the weakness. The "denial" condition in Wolfe et al. (2009) and the "low responsibility acceptance" condition in our paper are comparable in terms of the refusal to accept more responsibility.

(2009) by showing that, in an IT context, accepting more responsibility is not always more effective than accepting less responsibility; in fact, in Experiment 2, we find that low responsibility acceptance can be more effective than high responsibility acceptance with an internal breach. Specifically, in their experiment, the IT control deficiencies involved *external* parties (a notebook was stolen with the password stored inside; an intruder stole customer procurement card information). Therefore, their finding that a concession as opposed to a denial leads to lower auditor assessment of the deficiency significance for IT control deficiencies (both cases are external breaches) is consistent with our result in Experiment 1 that high (as opposed to low) responsibility acceptance leads to more favorable outcomes with an *external* breach. Moreover, our Experiment 2 further refines their "IT-diluting-blame" theory by showing that accepting high responsibility can invite blame that offsets or even outweighs the blame that is diluted by the IT element, making high (as opposed to low) responsibility acceptance a less effective communication strategy.

Our framework can also explain results in the textual disclosure condition in Elliott, Hodge, and Sedor (2012). Elliott et al. (2012) examine the effect of CEO's responsibility acceptance (via video or text) on investors' decisions. The responsibility acceptance/denial variable is manipulated as: "(w)e are *fully responsible/not responsible* for this error because we relied on the advice of our *internal/external* lease accounting expert when preparing our financial statements" (Elliott et al. 2012, 521, emphasis added). This manipulation involves two constructs. The "internal/external lease accounting expert" element in Elliott et al. (2012) is comparable to the breach variable (i.e., the "internal/external hacker") in our study in the sense that both describe whether the adverse event is associated with an internal staff or an outsider. The "responsibility acceptance/denial" element in Elliott et al. (2012) is comparable to the

responsibility acceptance variable in our study. Therefore, their responsibility acceptance condition is actually equivalent to our high responsibility acceptance/internal breach condition, and their responsibility denial condition is equivalent to our low responsibility acceptance/external breach condition. Elliott et al. (2012) find no effect of responsibility acceptance in the textual disclosure condition. This result is consistent with our finding that there is no difference in investment willingness between the high responsibility acceptance/internal breach condition and the low responsibility acceptance/external breach condition. We further extend Elliott et al. (2012) by separately manipulating the two elements in their responsibility acceptance condition—the amount of responsibility that management accepts and whether the event is associated with an internal or external party. We find that responsibility acceptance does matter in a textual disclosure, with the direction of the effect conditional on whether the related cause is internal or external.

The rest of the paper is organized as follows. Section II develops our hypotheses. Section III and IV provide details of Experiments 1 and 2, respectively. Section V reports the archival tests. Section VI concludes.

II. THEORY AND HYPOTHESIS DEVELOPMENT

Management's Responsibility Acceptance

Responsibility acceptance is one dimension generally included when people provide explanations about adverse outcomes. Such explanations are strategies to manage the impressions on their prior actions (Scott and Lyman 1968). According to account theory, the various types of explanations can be classified into four categories: concession, justification, excuse, and denial (Scott and Lyman 1968; Schonbach 1990). These four categories can be organized into a 2 × 2 matrix framework. The first dimension centers on whether or not the actor

admits the harm of an act, and the second consists of whether or not the actor admits responsibility. When both are admitted, the account is a concession, while denial of both constitutes a denial. Admitting responsibility but not harm equates to a justification, and the opposite condition is an excuse (see Figure 1).

[Insert Figure 1 about here]

In the context of internal control weakness disclosures, management does not have much discretion in the harm admission dimension, since management is not allowed to deny the existence of internal control weaknesses and the potential harm to the company when a breach occurs (SEC 2003); [4] hence, justification and denial are precluded from management's strategy set. Choices, although limited, exist on the responsibility admission dimension. Because regulations prescribe management's responsibility for maintaining an effective internal control system, management is not able to completely deny their responsibility when a breach occurs. However, management can choose the amount of responsibility to accept—a large proportion of responsibility (equivalent to a concession in Figure 1) or a small proportion of responsibility (equivalent to an excuse in Figure 1). By default, taking only a small amount of responsibility (i.e., an excuse) implies the need for a reason. One such reason management can use is the notion of "reasonable assurance." According to the COSO framework, "(a)n internal control system, no matter how well conceived and operated, can provide only reasonable—not absolute—assurance to management and the board regarding achievement of an entity's objectives" (COSO 1992, 6). The purpose of emphasizing the reasonable assurance concept is to remind financial statement users of the limitations inherent in every internal control system, no matter how well it is designed and operated. However, the ambiguity of the definition and scope of reasonable

[4] According to SEC's implementation guidance,"(m)anagement will be unable to conclude that the company's internal control over financial reporting is effective if there is one or more material weaknesses in such control" (SEC 2003, 1).

assurance[5] enables management to exploit the reasonable assurance statement as a means to reduce management's own responsibility. Appendix A provides examples for both strategic (low responsibility acceptance) and non-strategic (high responsibility acceptance) use of the reasonable assurance statement.

Social psychological research has investigated the efficacy of responsibility acceptance as an impression management tactic and finds mixed results. While some studies find that high responsibility acceptance reduces negative outcomes (e.g., penalties, perceived severity, blame, and anger) of an offence (Darby and Schlenker 1982; Snyder and Higgins 1988; Schonbach 1990; Bies and Sitkin 1992; Dunn and Cody 2000), other studies find that low responsibility acceptance (i.e., making excuses) reduces personal responsibility and generates more favorable outcomes (Crant and Bateman 1993; Wood and Mitchell 1981; Rosenfeld, Giacalone, and Riordan 1995). The mixed finding indicates both benefits and costs of high/low responsibility acceptance. High responsibility acceptance shows a person's integrity, trustworthiness, and reliability, which are desirable attributes and are valued by society at large (Goffman 1971). In addition, it also indicates an intention to remediate the problem and to avoid similar ones in the future (Bottom, Gibson, Daniels, and Murnighan 2002). However, high responsibility acceptance likely invites blame and increases the perceived responsibility for an adverse event. On the other hand, low responsibility acceptance has the benefit of weakening perceived personal responsibility. However, it has the cost of indicating the lack of integrity and unwillingness to remediate the problem if the excuses sound invalid or unconvincing (Schlenker et al. 2001; Tyler and Feldman 2007). Therefore, the efficacy of responsibility acceptance depends on whether the

[5] The PCAOB defines reasonable assurance as a high level of assurance, "understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis" (PCAOB 2007, 7). The SEC recognizes that while "reasonableness" is an objective standard, there is a range of judgments that an issuer might make as to what is "reasonable" in implementing Section 404 and the Commission's rules (SEC 2003). An auditor commented that "(t)he term 'reasonable assurance' leaves much to the imagination" (Goldwasser 2005, 28).

situation amplifies the benefits or costs of high/low responsibility acceptance. We posit that one such situational factor is the locus of breach.

Locus of Breach and the Triangle Model of Responsibility

We borrow the term "locus" from the term "locus of causality" in attribution theory (Heider 1958; Rotter 1966; Weiner 1985). In this literature, "locus of causality" refers to whether the cause of an outcome is internal (i.e., attributable to the person) or external (i.e., factors outside the person).[6] Similarly in our paper, "locus of breach" (or "breach") refers to whether the breach is from within (e.g., a sales representative hacking into the company's computer system) or outside (e.g., an outsider hacking) the company.[7] The negative outcome in the example refers to the consequence (e.g., change of sales orders) associated with the breach.[8]

Conceptually, locus of breach is different from responsibility assignment. For instance, Shaver and Drown (1986) specifically point out that studies on attribution of blame need to make a clear distinction between the constructs of responsibility and attribution of causality.[9] Various early models of responsibility assignment exist (e.g., Heider 1958; Hamilton 1978). The more current view is the triangle model of responsibility (Schlenker et al. 1994) which provides an integrative framework with linkages among the key determinants of responsibility assignment. According to this model, the responsibility assigned to an actor is a direct function of the strength of three linkages between the actor, the event, and the relevant prescriptions governing

[6] Internal causes are factors within the person (effort, ability, intention, etc.), while external causes are situational factors outside the person (task difficulty, luck, etc.) (Weiner 1985).

[7] We employ the "locus" concept in an organizational setting. The "locus" concept in our study refers to whether a breach is external or internal to the "company," rather than to the "manager."

[8] The negative outcome occurs when two conditions are present: (1) existence of the control weakness, and (2) occurrence of the breach. Note that the mere existence of a control weakness does not necessarily lead to a negative consequence. As stated in Auditing Standard No. 5, "(a) material weakness in internal control over financial reporting may exist even when financial statements are not materially misstated" (PCAOB 2007, A1-4). Similarly, a breach alone cannot result in a negative outcome if there is no underlying control weaknesses.

[9] Shaver and Drown (1986) review papers on self-blame, and indicate that conclusions from these studies are inconclusive because the concepts of responsibility, causality, and blameworthiness are not adequately distinguished in these studies.

it. The three linkages are (a) prescription clarity: whether the prescriptions (goals, rules, and scripts) that are applicable in the situation are ambiguous, linking the prescription and the event (Link 1); (b) personal obligation: the extent to which the prescriptions are perceived as being applicable to the actor because of duty or other requirements, linking the prescriptions and the actor (Link 2); and (c) personal control: the extent to which the actor seems to have control over outcomes in the situation, linking the actor and the event (Link 3; see Figure 2, Panel A). People are seen to be more responsible when prescriptions governing the event are clear, when they seem to have an obligation to behave in the prescribed ways, and when they are perceived to have personal control over the relevant event.

[Insert Figure 2 about here]

In the internal control disclosure setting, "event" refers to the breach of an internal control, "actor" refers to firm managers, and "prescriptions" refers to explicit codes and rules for the maintenance of a good internal control system, and/or the public's implicit expectations and norms. Link 1 relates to prescription clarity, which is the link between rules and/or public expectations/norms and the breach. We predict prescription clarity to be stronger in the external breach situation than in the internal breach situation. Guidance from professional bodies (e.g., IIA 2008) and professional frameworks (e.g., COSO 1992, Auditing Standards No. 5, PCAOB 2007) emphasizes the importance of an effective control system in preventing breaches (thus establishing prescription clarity), but explicitly recognizes that an inherent limitation in internal control systems is that controls can be circumvented by insiders (thus weakening this prescription in the case of internal breaches). Hence, while standard setters/professional bodies make explicit prescriptions about the important role of internal control systems, they also explicitly weaken this prescription in the case of internal breaches, suggesting that prescription

clarity is weaker in the latter. In terms of public expectations/norms, security attacks of high-profile organizations (e.g., Target Corporation, Sony Pictures) are commonly made by external parties (Verizon 2015), [10] and the need for greater information security are also widely publicized by the media. Hence, both the threat of external party attacks and the need for protection against these attacks are likely salient in the public's eyes. Media reports (e.g., Michaels 2014) of actions taken by the regulators to investigate the internal controls of the victims of these attacks (e.g., Target Corporation), which generally are by external parties, reinforce perceptions of regulatory concern for external breaches as opposed to internal breaches. Overall, we expect that prescription clarity (relating to the link between the breach and rules relating to maintaining good internal controls/public perceptions of norms) to be stronger for an external breach than for an internal breach.[11]

Link 2 relates to personal obligation—the extent to which the prescriptions relating to the maintenance of a good internal control system are perceived to be applicable to the actor because of duty or other requirements. We expect this link to be equally applicable in both external and internal breach situations. Managers are custodians and agents of the firm, and the maintenance of a good internal control system is likely unequivocally perceived to be their role and not that of another party, a role that is not contingent on whether actual/potential breaches are caused by internal or external parties. Regulators have made this management role very clear in their communications. Section 302 and 404 of SOX state that it is management, specifically the CEO/CFO, who is responsible for the adequacy of internal controls. For example, Section 302 requires that "the signing officers are responsible for establishing and maintaining internal

[10] The Data Breach Investigations Report by Verizon (2015) indicates that in terms of information security breaches, external as opposed to internal parties were responsible in over 80 percent of the cases every year between 2010 and 2014.

[11] Guidance from professional bodies (e.g., IIA 2008) and professional frameworks (e.g., COSO 1992, Auditing Standards No. 5, PCAOB 2007) recognizes that control effectiveness can be lower against internal (as opposed to external) threats, suggesting that Link 1 is viewed to be stronger for external than internal breaches in their eyes.

controls" (U.S. House of Representatives 2002, 777), and Section 404 specifies the need to "state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting" in an internal control report (U.S. House of Representatives 2002, 789). Thus, in both internal and external breach situations, regulators maintain that management is identified as the party responsible for setting up an effective internal control system.

Link 3 relates to personal control, relating to the link between the management (actor) and the breach (event). We expect this link to be stronger in external breach situations than in internal breach situations. A breach is deemed to be uncontrollable by management if management's voluntary actions cannot effectively prevent the occurrence of a breach. Breaches of an internal control by parties inside a company may be more difficult to prevent, and therefore are less controllable than those by parties outside a company. Access controls, password policies, and boundary protection of cyber-assets, which are common controls, are targeted more at outsiders. Such controls, even if implemented well, are effective against outsiders but are less effective in terms of preventing attacks by insiders (Upton and Creese 2012).[12] For instance, a company can have in place good controls that safeguard cyber-assets. A robust internal control system should be expected to protect physical or data thefts from external parties, but collusion and override of internal controls by insiders can thwart even the best system. A survey of global retailers (Bamfield 2010) reports that employee theft is more difficult to prevent than customer theft. Anecdotal evidence also shows that collusions among employees are hard to prevent and detect (Summerour 2002). Consistent with the COSO framework's stand that internal controls can be circumvented by members of a company, an internal breach situation (e.g., a hacking by

[12] Boundary protection, a common control for safe-guarding a company's assets, creates a "perimeter" around the company's assets. It is a defense against possible attacks by outsiders but not insiders.

an employee) is more difficult for management to prevent and control than an external breach situation (e.g., a hacking by an outsider). Thus, management controllability is higher in the external breach situation than in the internal breach situation.

To summarize, locus of breach affects responsibility assignment. Links 1 and 3 are stronger with an external breach than with an internal breach; Link 2 is equally strong with both breaches (see Figure 2, Panel B). Below, we discuss how locus of breach along with responsibility acceptance jointly affect responsibility assignment.

Interaction between Responsibility Acceptance and Locus of Breach

Psychological research shows that low responsibility acceptance (e.g., making excuses) can weaken the links in the triangle model and therefore reduce the actor's perceived responsibility for an adverse event (Schlenker et al. 2001). Researchers further find that the effect of low (as opposed to high) responsibility acceptance is moderated by the validity of the arguments; namely, whether or not the arguments are perceived to be believable and persuasive. For example, Tyler and Feldman (2007) find that excuses are more effective in reducing personal responsibility when they are more believable and show intensions of future correction and caring for other people. Barton and Mercer (2005) document that management's external explanation (i.e., excuses) for poor financial performance leads to higher earnings forecasts only when such explanation is perceived by analysts to be plausible and that it backfires when the explanation is perceived to be implausible.

As we discussed above, in an internal control weakness setting, management can accept low responsibility by employing the reasonable assurance argument, which emphasizes the inherent limitations of internal control systems. This argument weakens the prescription-event link by stating that the prescriptions (e.g., regulation, standards, norms, etc.) may not apply to certain

cases that are beyond the normal expectation. It also weakens the actor-event link because it implies that certain breaches may be beyond management's control. This argument is more effective in an internal (as opposed to external) breach situation, where breaches come from inside the company and are difficult to detect and prevent (as we discussed in the previous section). In other words, the features associated with internal (as opposed to external) breaches are more consistent with the message conveyed in the reasonable assurance argument. Meanwhile, this consistency suggests that the reasonable assurance argument is valid and believable and therefore, attenuates the negative implications associated with low responsibility acceptance. As a result, in the internal breach situation, low responsibility acceptance is likely more effective in reducing management's responsibility compared with high responsibility acceptance.

On the other hand, in an external breach situation, the reasonable assurance argument no longer applies because the breach comes from outside the company and is perceived to be more expected and controllable by the management (compared to internal breaches). The inconsistency between the reasonable assurance argument and the external breach situation casts doubt on the believability and validity of such arguments. Compared with low responsibility acceptance, the advantages (e.g., indication of integrity and future remediation) of high responsibility acceptance become more apparent in this situation. Therefore, we predict that, in the external breach situation, high responsibility acceptance is more effective in reducing management's responsibility for the breach.

H1: In the presence of an external (internal) breach, investors assign less (more) responsibility to management when management accepts more rather than less responsibility.

Investment Willingness

We expect the effects on responsibility assignment predicted in H1 to apply to investors' willingness to invest in the company for two reasons. First, when investors assign more responsibility to management for an internal control failure, they likely believe that material misstatement of the company's financial statements may not be prevented or detected on a timely basis. A potentially less reliable internal control system implies that controls that safeguard the assets of the company or the reliability/validity of accounting numbers generated within the company may be questionable. Consequently, investors may consider the company to be a less appropriate investment vehicle. Prior studies have demonstrated a negative association between the existence of internal control weaknesses and firm investment (Hammersley, Myers, and Shakespeare 2007; Rose, Norman, and Rose 2010).

Second, investors likely question management's credibility when they deem management responsible for control issues. Investors may question management's competence and trustworthiness in terms of effectively running the entire company. They may also experience negative emotions such as disappointment and anger while assigning responsibility to management. Both credibility assessment (Mercer 2005; Yang 2012) and affective reactions (Elliott, Jackson, Peecher, and White 2014) have impacts on investors' judgment and decisions. In summary, we predict that responsibility acceptance and breach interactively affect investment willingness in a manner similar to their effects on responsibility acceptance.

H2: In the presence of an external (internal) breach, investors are more (less) willing to invest in the firm when management accepts more rather than less responsibility for the internal control failure.

III. EXPERIMENT ONE

Participants

Our participants were seventy-eight M.B.A. students from two large universities in Singapore. The participants had an average working experience of 7.27 years. Fifty-five percent of the participants were male. We randomly assigned participants to experimental conditions. M.B.A. students are valid proxies for general investors as they have basic knowledge of accounting, business finance, and financial markets to respond meaningfully to our materials (Elliott, Hodge, kennedy, and Pronk 2007).

Experimental Design and Independent Variables

We employed a 2 × 2 between-subjects design with Breach (internal, external) and Responsibility Acceptance (low, high) as independent variables. All participants received the management's report on internal control over financial reporting which stated that "(t)here was a failure to maintain adequate access controls over the sales recording system." We use an information technology (IT) breach setting, consistent with the scenarios used in Wolfe et al. (2009) and Rose et al. (2010). In the manipulation of *external (internal)* breach, participants read the following:

> This material weakness resulted from *an outsider* (*a sales representative*) hacking into the computer system and changing the sales orders.

Responsibility acceptance was manipulated by varying the extent to which management accepted their responsibilities for the hacking incident. In the low responsibility acceptance condition, participants read the following: [13, 14, 15]

[13] We assessed whether participants have similar perceptions about the scope of reasonable assurance by asking this question: "Do you think the hacking instance described in the case is within or outside the scope of reasonable assurance?" (where -5 = within reasonable assurance, and 5 = outside reasonable assurance). The mean response is 0 in the high responsibility acceptance condition, and -0.3 in the low responsibility condition; the difference is not

> A control system, no matter how well conceived and operated, can provide only reasonable rather than absolute assurance that the objectives of the control system are met. Our management team is of the opinion that no control system can provide absolute assurance that all control issues (including this hacking instance) will be detected.

In contrast, participants in the high responsibility acceptance condition read the following:

> A control system should be well conceived and operated to provide reasonable (not absolute) assurance that the objectives of the control system are met. Our management team acknowledges the responsibility to ensure that our control system should provide reasonable assurance that control issues (including this hacking instance) will be detected.

Procedure

The experiment was completed under controlled conditions and under the supervision of an experimenter. Participants were provided with the background information of a hypothetical firm, selected financial data of the firm, the management's report on internal control over financial reporting, and a series of questions. Participants assumed the role of a general investor in all conditions. The background information of the hypothetical firm, Griffin Inc., was adapted from Wolfe et al. (2009). Griffin Inc. was a typical manufacturing company. The selected financial data and the stock price history showed a slow but steady growth, creating a favorable impression of the firm and its investment attractiveness prior to the control weakness disclosure.

After reading the background information of the firm, participants received the

---

significant (p=0.68). This result suggests that it is unlikely that the effect of responsibility acceptance is due to investors' different perceptions about the scope of reasonable assurance across conditions.

[14] We did not directly manipulate the absence versus presence of responsibility acceptance due to the restriction inherent in the internal control reporting setting. Specifically, Section 302 and 404 of SOX clearly prescribe management as the primary party responsible for maintaining an effective internal control system (U.S. House of Representative 2002). Therefore, it is unlikely that management can *completely* deny their responsibility for a breach in an internal control report. Further, based on our sample internal control reports from 292 firms, we observe that management varies the amount of responsibility that they are willing to accept by using the "reasonable assurance" statement.

[15] We asked participants the extent to which they perceived management's explanation to be defensive on an 11-point scale (0 = not defensive at all; 10 = extremely defensive). The mean response is 5.33 for the high responsibility acceptance condition and 6.06 for the low responsibility acceptance condition; the difference is insignificant (p=0.169). This result suggests that a defensive tone cannot explain the difference between the high and low responsibility acceptance conditions.

management's report on internal control over financial reporting described in Auditing Standard No. 5 (PCAOB 2007). Participants were told that there was a material weakness—a failure to maintain adequate access controls over the sales recording system in the corresponding reporting period. The reports were identical across all experimental conditions, except for the breach and responsibility acceptance manipulations.

We chose material weaknesses rather than other types of weaknesses because of two reasons. First, the main purpose of internal control is to identify any material weakness. As stated in the SEC Staff Statement, "the overall focus of internal control reporting should be on those items that could result in material errors in the financial statements" (SEC 2005). Second, the disclosure of material weaknesses has significant capital market consequences (Ogneva, Subramanyam, and Raghunandan 2007; Hammersley et al. 2007; Palmrose, Richardson, and Scholz 2004).

Across all conditions, participants were told that management will take further remediation efforts during the next fiscal year. Hence, management's intention to rectify the weakness remains identical in all conditions. Following Rose et al. (2010), participants are also informed that an independent auditor conducted its own evaluation of the firm's internal control over financial reporting and identified the same control problem. Hence, there is no conflict between the findings of management and the auditor. Participants then made several assessments about the firm, including questions on investment willingness and responsibilities assigned to management. Finally, participants answered manipulation check and debriefing questions.

Dependent Variables

To examine how investors assigned responsibilities to management, we asked participants the following question, "How much responsibility do you think the management

should take for the internal control failure?" (where 0 = no responsibility, and 10 = all responsibility). We used the average of the following two questions to measure investment willingness: (1) "How willing are you to invest in Griffin's stock?" (where 0 = absolutely not willing to invest, and 10 = absolutely willing to invest), and (2) "Suppose you hold Griffin's stock. How will you change your holdings of Griffin's stock?" (where -5 = significantly decrease, 0 = no change, and 5 = significantly increase). Cronbach's Alpha for the two questions is 0.74, above the 0.70 cutoff (Cortina 1993).[16]

Manipulation Checks

To assess the effectiveness of our responsibility acceptance manipulation, we asked participants the following question: "To what extent is Griffin's management taking responsibility for the hacking incident?" (where -5 = deny responsibility, and 5 = accept responsibility). The mean response in the high responsibility acceptance condition is 1.60, significantly higher than the mean response (0.21) in the low responsibility acceptance condition (p=0.02),[17] suggesting a successful manipulation of responsibility acceptance. To assess the effectiveness of our breach manipulation, we asked participants to identify whether the material weakness results from an outsider or a sales representative hacking into the computer system. Eighty-six percent of participants correctly answered this question. [18]

Tests of Hypotheses

H1 predicts that in the presence of an external (internal) breach, investors assign less (more) responsibility to management when management accepts more rather than less responsibility. We conduct an ANOVA to analyze the interactive effect of breach and

[16] The second question was converted to a 0-10 scale to be combined with the first measurement. We obtain similar results when we analyze each question separately.
[17] All p-values are two-tailed, unless otherwise specified.
[18] We excluded 11 participants who failed this question for the subsequent analyses. Results are qualitatively similar if we use responses from all participants.

responsibility acceptance on responsibility assigned to management. Table 1 reports the descriptive statistics and ANOVA results. Figure 3, Panel A illustrates the results. We find a significant interactive effect (p=0.03, one-tailed). Specifically, we find that in the presence of an external breach, the mean assessment in the high responsibility acceptance condition (mean=8.11) is marginally significantly lower than that in the low responsibility acceptance condition (mean=9.00; p=0.06, one-tailed). In the presence of an internal breach, the mean assessment in the high responsibility acceptance condition (mean=8.67) is higher than that in the low responsibility acceptance condition (mean=8.13), but the difference is insignificant (p=0.17, one-tailed). Thus, our results only partially support H1.

[Insert Table 1 and Figure 3 about here]

H2 predicts a similar pattern for investment willingness. We conduct an ANOVA with breach and responsibility acceptance as the independent variables and investment willingness as the dependent variable (see Table 2 and Figure 3, Panel B). The ANOVA results show a significant interactive effect on investment willingness (p=0.01, one-tailed). Specifically, in the presence of an external breach, investors' mean willingness to invest is 4.63 in the high responsibility acceptance condition, significantly higher than the mean of 3.00 in the low responsibility acceptance condition (p=0.02, one-tailed). In the presence of an internal breach, investors' mean willingness to invest is not significantly different between the high and low acceptance conditions, although the means are directionally consistent with our prediction (means=3.72 and 4.50, respectively; p=0.13, one-tailed). Again, our results only partially support H2. [19, 20]

[19] We also conducted a within-subjects test following the between-subjects test. Participants read excerpts from four different companies' internal control reports on the same page simultaneously, with each excerpt representing one of our treatment conditions. We do not find any interaction effect of breach and responsibility acceptance on either investment willingness or responsibility assignment (p>0.35). However, the main effect of breach is significant for

[Insert Table 2 about here]

We also assess the simple main effects of breach, at each level of responsibility acceptance (see Table 1, Panel C and Table 2, Panel C). With low responsibility acceptance, investment willingness is significantly higher in the presence of an internal rather than external breach (means=4.50 and 3.00, respectively; p=0.04). However, the simple effect of breach on investment willingness with high responsibility acceptance is insignificant (p=0.18). Together, these results suggest that the different effects between high and low responsibility acceptance at each level of breach result primarily from the *low* responsibility acceptance condition.

Supplemental Analyses

Test of the Triangle Model of Responsibility

To test Link 1 of the triangle model of responsibility (prescription clarity; see Figure 2), we asked participants this question: "Do you think that current regulations clearly prescribe the need to maintain an effective internal control system?" (where 0 = not at all clear, and 10 = extremely clear). The mean response in the external breach condition is 6.27, significantly higher than the mean response in the internal breach condition 5.21 (p = 0.05, one-tailed), suggesting that participants perceive prescriptions to be more clearly stated for external threats than for

---

both the investment willingness and responsibility assignment variable (both p<0.01), with external breaches leading to more favorable outcomes than internal breaches. The main effect of responsibility acceptance is significant only for the investment willingness variable (p<0.01), with high (as opposed to low) responsibility leading to more investment; the main effect of responsibility acceptance is insignificant for the responsibility assignment variable (p=1.00). The different pattern of results between the within- and between-subjects tests suggests that the between-subjects effects may be unconscious.

[20] We conducted a separate experiment to test whether a direct denial of responsibility leads to similar results as our main experiment. Participants were 28 M.B.A. students from a major university in the U.S. We utilized a 1× 2 between-subjects design with responsibility acceptance (high vs. denial) as the independent variable, with both cells set in the original external breach condition in Experiment 1. In the denial condition, participants are told that "(a) control system should be well conceived and operated to provide reasonable (not absolute) assurance that the objectives of the control system are met. Our management team does not take the responsibility to ensure that our control system can provide assurance that all control issues (including this hacking instance) will be detected." The high responsibility acceptance condition is equivalent to that used in our main experiment. We find that high responsibility acceptance leads to marginally more favorable evaluations (i.e., higher perceived credibility of management, p=0.07, one-tailed; and lower perceived misstatement likelihood, p<0.08, one-tailed) and investment decisions (p=0.04, one-tailed) than a denial of responsibility.

internal threats. To test Link 2 (personal obligation), we asked participants this question: "Do you think that current regulations clearly prescribe the management as the primary party responsible for internal control failures such as this hacking instance?" (where 0 = not at all clear, and 10 = extremely clear). The mean responses in the external and internal breach conditions are 4.82 and 4.53, respectively, and not significantly different (p=0.65). To test Link 3 (personal control), we asked participants this question: "How much control does Griffin's management have in preventing this internal control weakness?" (where 0 = no control, and 10 = a lot of control). The mean response in the external breach condition is 7.52, significantly higher than the mean response of 6.47 in the internal breach condition (p = 0.04, one-tailed).[21] These results support the hypothesized links in the triangle model of responsibility. [22]

Test of Alternative Explanation—Severity

An alternative explanation to our study is that it is the perceived severity of the internal control weakness, rather than its locus of breach, that moderates the effect of management's responsibility acceptance. For instance, it is conceivable that a weakness that occurs in the external breach condition is deemed to be more serious than one that occurs in the internal breach condition. To rule out this alternative explanation, we tested whether participants perceived the severity of the weakness to be different between the external and internal breach conditions, on a scale of 0 (not severe at all) to 10 (extremely severe). The mean rating for severity is 6.79 for the external breach condition and 7.18 for the internal breach condition. The difference is insignificant (p=0.50), indicating that participants perceived the weakness with both

[21] An additional analysis indicates that personal control (either as an interval variable or dummy variable from a median split) does not interact with breach (internal, external) to influence responsibility assignment (p > 0.76).

[22] Another question that we asked to test Link 3 is the following: "Could Griffin's management have predicted this internal control weakness in advance?" (where 0 = not at all predictable, and 10 = extremely predictable). The mean response in the external breach condition is 6.42, marginally higher than the mean response of 5.74 in the internal breach condition (p=0.10, one-tailed). We did not average the responses to these two questions (i.e., the controllability question and the predictability question) because Cronbach's Alpha of these two questions is 0.59, lower than the 0.70 cutoff of reliability.

breaches to be similarly severe. An ANOVA test detects neither main nor interaction effects (smallest p=0.50). This result also precludes the possibility that severity mediates the effect of the manipulated variables on either responsibility assignment or investment willingness. Therefore, severity cannot explain the interactive effects of breach and responsibility acceptance.

Test of Process

We investigate the process through which responsibility assignment affects investment willingness. We conjecture that responsibility assignment affects investment willingness through two mediators—investors' assessment of the misstatement likelihood and their impression of management. According to the SEC's guidance regarding management's report on internal control over financial reporting, management has the duty to identify and prevent the risks of material misstatement (SEC 2007). In our setting, when investors assign more responsibility to management, investors likely believe that management did not fully perform its duty; as a result, the likelihood of misstatement increases. The increased likelihood of misstatement has both direct and indirect effects on investment willingness. On the one hand, prior research finds that the increased likelihood of misstatement leads to negative market reactions (Palmrose et al. 2004). On the other hand, the increased likelihood of misstatement can leave a negative impression of management on investors, which in turn affects investors' investment decisions (an indirect effect). Investors may have negative impressions of management in multiple ways. For instance, investors may have doubts on management's credibility. Alternatively, investors may have negative affective reactions towards management.

To make our model more parsimonious, we performed a principle component analysis on the questions measuring management's credibility and investors' affective reactions.[23] We find

[23] Credibility was measured as the average of responses to three questions, each measuring management's competence, honesty, and trustworthiness, respectively (Mercer 2005). These three questions were measured using

that one latent factor accounts for the majority of the variance (eigenvalue=1.56, variance explained=78 percent). We name this latent factor "impression of management." Next, we conducted a structural equations-based path analysis using SPSS-AMOS software, which allows a simultaneous analysis of multiple regressions (Kline 1998). Figure 4 presents the structure of our process model. This model has adequate fit, with comparative fit index (CFI) = 0.98, and the root mean square error of approximation (RMSEA) = 0.06 (Kline 1998). [24] We find that the interaction term of our two manipulated variables (responsibility acceptance and breach) has a significant direct effect on responsibility assignment (coefficient=-0.40, p=0.03, one-tailed), which supports H1. Consistent with our conjecture, responsibility assignment has a direct effect on misstatement likelihood (coefficient=0.23, p=0.03, one-tailed); misstatement likelihood directly influences both impression of management (coefficient=-0.33, p<0.01, one-tailed) and investment willingness (coefficient=-0.27, p<0.01, one-tailed); and impression of management has a direct effect on investment willingness (coefficient=0.71, p<0.01, one-tailed). We also find an unexpected link from the interaction of responsibility acceptance and breach to impression of management (coefficient=0.39, p=0.04) (see Table 3, Panel A). The direct, indirect and total effect of each variable on investment willingness is summarized in Table 3, Panel B.

[Insert Table 3 and Figure 4 about here]

IV. EXPERIMENT TWO

Motivation and Design

Results from Experiment 1 only partially support our hypotheses in that we found

11-point scales from 0 to 10 (Cronbach's Alpha=0.75). Affect was measured as the average of responses to three questions, each measuring investors' feelings of happiness, satisfaction, and angry, respectively (Elliot et al. 2014). These three questions were measured using 11-point scales from 0 to 10 (Cronbach's Alpha=0.76). Responses to the question on angry were reverse-ordered before aggregation. We measured misstatement likelihood using an 11-point scale from 0 to 10.

[24] According to Kline (1998), a CFI of 0.95 (0.90) or more and a RMSEA of 0.05 (0.08) or less indicate good (adequate) fit of the model.

significant effects of responsibility acceptance only in the external breach condition but not in the internal breach condition. We posit that the insignificant results in the internal breach condition likely result from certain weaker links of the triangle model. As explained earlier, the prescription-event link is weaker for internal than external breaches because external breaches receive more regulatory and media attention than internal breaches. Similarly, the actor-event link is weaker for internal than external breaches because insiders can more easily circumvent or override internal controls through collusion and insider knowledge. Psychological research finds that excuses are more effective in reducing personal responsibility only when the links of the triangle model are strong rather than weak (Tyler and Feldman 2007). Therefore, a logical prediction is that we would be able to find a more significant effect of responsibility acceptance with stronger triangle-model-links within the internal breach condition. We designed Experiment 2 with this in mind. Specifically, we employed a 2 × 2 between-subjects design with Link Strength (strong, weak) and Responsibility Acceptance (high, low) as the independent variables. All the four conditions utilized the original *internal* breach setting. The Responsibility Acceptance variable was manipulated the same way as in Experiment 1. In the strong-link condition, we added the following statement which clearly prescribed that companies need to implement measures to guard against internal breaches: "(a)n authoritative computer security report recently warned companies against being complacent about their internal control systems as these can be easily circumvented by insiders, and advised companies to implement measures to guard against the possibility of hacking by their own employees" (see Appendix B). This statement strengthens the prescription-event link within this internal breach setting by reminding readers that the onus is on management to safeguard against insider control breaches. In addition, the actor-event link is also strengthened because management should have preempted and

prepared themselves for possible instances of hacking or internal breaches. The above paragraph was absent in the weak-link condition. Therefore, the weak-link condition is equivalent to the original internal breach condition, while the strong-link condition is equivalent to the original internal breach conditions with stronger prescription-event and actor-event links. We predict that, within this internal breach setting, low responsibility acceptance in the strong-link condition leads to more favorable outcomes than high responsibility acceptance, and that the effect of responsibility acceptance remains insignificant in the weak-link condition.

Participants

Two hundred and twenty-eight workers from the Amazon Mechanical Turk (AMT) platform participated in this experiment. Participants' locations were restricted to the United States only. We selected this participant pool to test whether the results in Experiment 1 can be generalized to investors in the U.S., as well as investors with less professional training. Participants had an average working experience of 14.62 years. Sixty-six percent of the participants were male. On average, participants had taken 3.04 accounting courses, 2.08 finance courses, and 2.0 economics courses. In addition, 95 percent reported that they had investment experience. These demographic statistics suggest that participants from the AMT are comparable to the M.B.A. students who participated in Experiment 1, with the former having even more working experience.

Participants went through the same procedures as in Experiment 1, reading similar case materials and responding to the same set of dependent variables. [25]

Results

[25] In Experiment 1, we described the breach in the case material as "(t)here was a failure to maintain adequate access controls over the sales recording system. This material weakness resulted from an outsider (a sales representative) hacking into the computer system and changing the sales orders." In Experiment 2, we changed this description to "(t)here was a failure to maintain adequate access controls over the sales recording system. Because of this access control weakness in the control system, the Company's sales recording system was breached." (see Appendix B) This new description was also utilized in the supplementary experiment described in footnote 20.

To assess the effectiveness of our manipulation of Link Strength, we asked participants to indicate the extent to which Griffin's management could have foreseen this security breach in advance (0 = not at all predictable; 10 = extremely predictable). The mean response in the strong-link condition (mean=6.50) is significantly higher than that in the weak-link condition (mean=6.00; p=0.02, one-tailed). To check the manipulation of the Responsibility Acceptance variable, we asked participants to assess the extent to which management was taking responsibility for the breach (0 = deny responsibility; 10 = accept responsibility). The mean response in the high acceptance condition (mean=6.88) is significantly higher than that in the low acceptance condition (mean = 5.20; $p<0.001$, one-tailed). These results show that our manipulations of Link Strength and Responsibility Acceptance are successful.

Using the same responsibility assignment measure as in Experiment 1, ANOVA results show a significant interaction between Link Strength and Responsibility Acceptance (p=0.03, one-tailed). Specifically, in the strong-link condition, participants assign significantly less responsibility to management when it takes less (mean=7.58) rather than more responsibility (mean=8.46; $p<0.01$, one-tailed). In the weak-link condition, however, participants assign similar responsibility to management whether management takes less (mean=7.86) or more responsibility (mean=7.89; p=0.92). This result is consistent with our prediction for Experiment 2 (see Table 4 and Figure 5, Panel A).

[Insert Table 4 and Figure 5 about here]

With respect to the investment willingness measure that we used in Experiment 1, ANOVA results show a significant interaction between Link Strength and Responsibility Acceptance ($p<0.01$, one-tailed). Specifically, in the strong-link condition, investors are more willing to invest in Griffin's stock when management accepts less (mean=4.87) rather than more

responsibility (mean=3.82; p<0.01, one-tailed). In the weak-link condition, the mean willingness is not significantly different between the low (mean=3.65) and high responsibility acceptance conditions (mean=4.20; p=0.20). Again, this result is consistent with our prediction for Experiment 2 (see Table 5 and Figure 5, Panel B). That the results for the weak-link condition here using AMT participants are similar to that for the internal breach condition in Experiment 1 using Singaporean M.B.A. participants provides evidence of the generalizability of our results. Further, the results in Experiments 1 and 2, together, indicate that the differential efficacy of responsibility acceptance between external and internal breaches cannot be simply explained by the strengths of the triangle-model-links, since the strong-link condition in Experiment 2 has links that are similarly strong to those in the external breach condition in Experiment 1 but we find opposite results. Therefore, it is the locus of breach, rather than the strengths of the triangle-model-links, that moderates the effect of responsibility acceptance on investors' judgment and decision-making.

[Insert Table 5 about here]

Supplemental Analyses

Management Credibility

As in Experiment 1, we measured management credibility by averaging the responses to three questions on management's competence, honesty, and trustworthiness, respectively. We combined the measures (Cronbach's alpha=0.86), and the ANOVA results indicate a significant interaction (p=0.03, one-tailed) and insignificant main effects of both responsibility acceptance (p=0.51) and link strength (p=0.12). Specifically, in the strong-link condition, the mean credibility rating is higher with low responsibility acceptance (mean=5.92) than with high responsibility acceptance (mean=5.27; p=0.03, one-tailed). In the weak-link condition, however,

the mean credibility ratings are similar across the low and high responsibility acceptance conditions (5.04 versus 5.37; p=0.37).

Affect

As in Experiment 1, we measured affect as the average of responses to four questions, each measuring investors' feelings of happiness, satisfaction, disappointment (reverse-coded) and anger (reverse-coded). We combined these measures (Cronbach's alpha=0.77), and the ANOVA results show a significant interaction (p=0.01, one-tailed) and insignificant main effects of both responsibility acceptance (p=0.13) and link strength (p=0.95). The interaction shows that, in the strong-link condition, participants experienced more positive affect when management's responsibility acceptance is low (mean=4.35) rather than high (mean=3.35; p<0.01, one-tailed). In the weak-link condition, however, the affect assessment is similar between the low and high responsibility acceptance conditions (3.72 versus 3.95; p=0.53).

Together, these findings support our theory that low (as opposed to high) responsibility acceptance reduces management's responsibility and leads to greater investment willingness in the presence of an internal breach. Our debriefing results further support this argument by showing that low (as opposed to high) responsibility acceptance leads to greater perceived credibility of management and more positive affect in the presence of internal breaches.

Investors' General Opinions towards Internal versus External Breaches

In the debriefing section, we obtained participants' general opinions about the preventability, detectability and the likelihood of re-occurrence between internal and external breaches on three 11-point scales (-5 = internal breaches are more difficult to prevent/detect/more likely to re-occur; 5 = external breaches are more difficult to prevent/detect/more likely to re-occur; 0 = no difference). The mean responses for each of the

three questions are -2.03, -1.91, and -1.07, respectively. All of these mean responses are significantly below 0 (all $p<0.001$). [26] This result shows that in general, investors perceive internal breaches to be more difficult to prevent and detect and more likely to re-occur in the future than external breaches.

V. ARCHIVAL TESTS

In order to generalize our experimental findings to real-life decision-making contexts, we coded 300 actual internal control reports and tested whether locus of breach and management's responsibility acceptance jointly affect market reactions. Specifically, we first selected all reports (n=5,251) containing material weaknesses between 2009 and 2011 in the Audit Analytics database.[27] Next, we matched the companies issuing these reports with those in the Center for Research in Securities Prices (CRSP) database that have permanent identifiers ("PERMNO") to link to market returns. The overlap resulted in 732 reports, among which we randomly selected 300, with 100 reports from each year.[28] We dropped eight observations with missing values. Therefore, our final sample consists of 292 observations. One author of the paper and a doctoral student independently coded these reports. The doctoral student was unaware of our hypotheses. Inter-rater agreement is 93 percent and discrepancies were resolved through discussion.

We coded the locus variable in terms of whether control weaknesses are related to internal factors (e.g., lack of segregation of duties) or external factors (e.g., statements prepared

[26] We asked the same questions in a separate survey conducted with 111 M.B.A. students from a large university in Singapore and also find that similar results. Investors believe that internal (as opposed to external) breaches are more difficult to prevent and detect and more likely to re-occur in the future, with no significant differences between the high and low familiarity groups (mean response for each of the three questions is -1.98, -2.73, and -1.69, respectively; each mean is significantly below 0 at $p<0.001$).

[27] We select the period 2009-2011 because it is the most recent period when the remediation data (in one to three years from the filing date of a report) is available, which are used in a separate study on the remediation of control weaknesses.

[28] Specifically, we assigned a sequence number (from 1 to 732) to each report and used the random-number-generating function in Microsoft Excel to generate 300 random, non-repeated numbers (100 numbers for each year). Reports were selected if their sequence numbers matched the random numbers.

by a third-party accounting firm). Our coding shows that the majority (229 or 78.4 percent) of the reports mention only internal factors (e.g., lack of segregation of duties), 45 (15.6 percent) reports mention both internal and external factors, three reports (one percent) mention external factors only (e.g., an outside expert), and 15 (5.1%) reports do not specify the factors related to the weaknesses. Since we are not interested in the "cause-not-mentioned" category of the locus variable, we exclude these observations for subsequent analyses. We reasoned that for the "internal-and-external" category, the external factors are probably salient given that the majority of the reports mention some internal factors; hence, we combined the "internal-and-external" category with the "external-only" category. We coded locus as 0 for reports that mention only internal factors, and 1 for reports that mention external factors (i.e., both "internal-and-external" and external-alone; see Appendix A for examples of each category).

We used three variables to capture our responsibility acceptance construct. The first variable is "responsibility statement," which is coded as 1 if the report contains the statement that "management is responsible for establishing and maintaining adequate internal control over financial reporting" or similar statements; 0 otherwise. The second variable is "non-strategic assurance," which is coded as 1 if the report contains a reasonable assurance argument that is not worded to fend off management's responsibility; 0 otherwise. The third variable is "strategic assurance," which is coded as 1 if the report words the reasonable assurance argument in a strategic fashion to reduce management responsibility; 0 otherwise. The descriptive results show that among our 292 reports, 278 (95.2%) contain the responsibility statement, 146 (50%) include the non-strategic reasonable assurance argument, and 83 (28.4%) include the strategic reasonable assurance argument.

We also coded whether the report mentioned remediation plans (0=absent; 1=present) and

the consequence of the weaknesses (0=no consequence; 1=adjustment; 2=restatement) as control variables. Following prior studies on the relation between internal control weaknesses and market reactions (e.g., Ogneva et al. 2007, Hammersley et al. 2008), we controlled for the number of weaknesses, Big-4 auditors (no, yes), market value, book/market ratio, whether there is a loss in earnings, and whether the dates of the earnings announcements coincide with the10-K filings. We used the reporting companies' cumulative abnormal returns (CARs) during the (-2, 2) window around the filing dates of the internal control reports as our dependent variable. [29] Table 6, Panel A reports the descriptive statistics, and Panel B reports the correlation matrix of the variables mentioned above.

We ran a linear regression with locus, the three variables measuring responsibility acceptance, as well as the control variables as the explanatory variables, and market returns as the dependent variable. Our regression model is as follows:

$$\begin{aligned} Market\ returns \\ &= \beta_0 + \beta_1 Locus + \beta_2 Responsibility\ statement \\ &+ \beta_3 NonStrategic\ assurance + \beta_4 Strategic\ assurance + \beta_5 Controls \end{aligned} \quad (1)$$

We find at least marginally significant coefficients on the responsibility statement (β_2 = -0.063, t = -1.83, p = 0.069) and strategic assurance variables (β_4 = 0.067, t = 3.16, p = 0.002; see Table 6, Panel C). The negative sign of β_2 and the positive sign of β_4 both indicate that market reactions are less negative when management accepts low rather than high responsibility. Economically, the cumulative returns in a (-2, 2) window decrease by 6.3 percent when managers accept more / full responsibility through the responsibility statement, and increase by 6.7 percent when managers strategically state the reasonable assurance argument to accept less responsibility. Note that using a non-strategic reasonable assurance argument does not have a

[29] We also ran our regression using returns in the (-1, 1) window but results are insignificant, presumably because investors need more time to capture and digest the message conveyed by an ICFR report out of a lengthy annual filing.

significant impact on market returns (β_3 = 0.032, t = 1.63, p = 0.105). These results are consistent with our finding in Experiment 2 that investor reactions are less negative when management accepts less rather than more responsibility in the presence of internal breaches, given that the majority (78 percent) of the reports mention only internal factors. As a further test, we retained only observations specifying internal factors, and ran Model (1) without the locus variable. We obtain similar findings. Untabulated results show that market returns are negatively associated with the responsibility acceptance statement variable (coefficient = -0.078, t = -2.08, p = 0.038), and positively associated with the strategic assurance variable (coefficient = 0.069, t = 2.94, p = 0.004). The coefficient on the non-strategic assurance variable is not significant (coefficient = 0.029, t = 1.34, p=0.182). We also ran another model where we added an interaction term between locus and the responsibility acceptance measures, but the interaction terms are not significant, possibly because of the skewed distribution of the locus variable.

[Insert Table 6 about here]

VI. CONCLUSION

This study investigates the joint effects of two aspects of management's explanations on investors' judgment: discussion of the amount of responsibility that management accepts for breaches of control weaknesses and the locus of such breaches. In Experiment 1, we find that in the presence of an external breach, investors assign less responsibility to management and are more willing to invest in the firm when management accepts more rather than less responsibility. In contrast, in the presence of an internal breach, the effect of responsibility acceptance is not significant. In additional analyses, we find support for the triangle model of responsibility. In Experiment 2, we document that with strengthened prescription-event and actor-event links in an internal breach setting, low (as opposed to high) responsibility acceptance leads to higher

investment willingness and lower responsibility assignment. Our archival results show that the market reacts less negatively when management accepts less (as opposed to more) responsibility for internal breaches. This result is economically significant.

This study has implications for researchers as it provides additional insights regarding the effects of managers' explanations on investors' judgment. We find that the efficacy of managers' explanation (i.e., high or low responsibility acceptance) is conditional on situational factors such as locus of breach. This finding complements prior research on management's explanations and provides a framework to integrate the results from prior studies. We extend Wolfe et al. (2009) by finding that accepting more responsibility is not always effective even for IT deficiencies; in fact, we find that accepting more responsibility can lead to worse outcomes in the case of internal breaches. We also add to Elliott et al. (2012) by disentangling the two elements in their responsibility manipulation—management's responsibility acceptance and the internal versus external party involved. We find that responsibility acceptance does have a significant effect in a textual disclosure, with the directional effect conditional on whether the related cause is internal or external.

Our study informs regulators and standard setters on how the "reasonable assurance" argument can be strategically used by managers as a defense to ameliorate investors' negative reactions to the disclosure of material weaknesses, and suggests perhaps the need for a better clarification to the public on what "reasonable assurance" means. This aspect is important because a majority (seventy-eight percent) of the ICFR reports in our archival sample emphasize the "reasonable assurance" aspect of internal control systems, among which thirty-six percent are stated strategically with the intent to fend off responsibility. Our archival results show that a strategic statement of reasonable assurance successfully reduces the market's negative reactions

toward the control failures.

Our study also has implications to managers. In our archival sample, a majority (seventy-eight percent) mention internal factors only. According to our findings in Experiment 2, in the case of an internal breach, high responsibility acceptance actually leads to worse outcomes than low responsibility acceptance. Therefore, our paper is informative to managers on possible investor reactions depending on the level of responsibility they accept in these situations.

Our paper has limitations. Firstly, our theory suggests that internal and external breaches differ in both the prescription-event and the actor-event links. Our paper is not able to distinguish which specific link drives the results as they have the same directional effects in our setting. Future research can examine the specific effects of each link in the triangle model, particularly when the links have differential strengths and/or go in opposite directions.

Secondly, our internal breach condition involves a staff committing a breach, and it can be argued that management has responsibility for hiring and monitoring employees. While our participants did not appear to penalize management for hiring staff with questionable ethics, it is possible that investors do care about this issue when it is apparent that management is to blame for adopting poor hiring policies. While the latter is an important dimension of management's overall responsibility, it is difficult to examine this dimension in the external breach condition, where employees are not the wrong-doers and management's hiring and monitoring responsibility does not apply. Future research can examine how our results are moderated when management's responsibility for hiring the culpable employee is considered.

REFERENCES

Alwin, D. F., and R. M. Hauser. 1975. The Decomposition of Effects in Path Analysis. *American Sociological Review* 40 (1): 37-47.

Bamfield, J. 2010. *The Global Retail Theft Barometer 2010: Monitoring the Costs of Shrinkage and Crime in the Global Retail Industry*. Nottingham: Center for Retail Research.

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

Bies, R. J., and S. B. Sitkin. 1992. Excuse-making in organizations: Explanation as legitimation. In *Explaining one's self to others: Reason giving in a social context*, edited by M. L. McLaughlin, M. J. Cody and S. Read. Hillsdale, N.J.: Lawrence Erlbaum Associates, 183-198.

Bottom, W. P., K. Gibson, S. E. Daniels, and J. K. Murnighan. 2002. When Talk Is Not Cheap: Substantive Penance and Expressions of Intent in Rebuilding Cooperation. *Organization Science* 13 (5): 497-513.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. *Internal Control-Integreated Framework*. Jersey City, NJ: AICPA.

Cortina, J. M. 1993. What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology* 78 (1): 98-104.

Crant, J. M., and T. S. Bateman. 1993. Assignment of Credit and Blame for Performance Outcomes. *Academy of Management Journal* 36 (1): 7-27.

Darby, B. W., and B. R. Schlenker. 1982. Children's reactions to apologies. *Journal of Personality and Social Psychology* 43 (4): 742-753.

Dunn, D., and M. J. Cody. 2000. Account credibility and public image: Excuses, justifications, denials and sexual harassment. *Communication Monographs* 67 (4): 372-391.

Elliott, W. B., F. D. Hodge, J. J. kennedy, and M. Pronk. 2007. Are M.B.A. Students a Good Proxy for Nonprofessional Investors? *The Accounting Review* 82 (1): 139-168.

Elliott, W. B., F. D. Hodge, and L. M. Sedor. 2012. Using Online Video to Announce a Restatement: Influences on Investment Decisions and the Mediating Role of Trust. *The Accounting Review* 87 (2): 513-535.

Elliott, W. B., K. E. Jackson, M. E. Peecher, and B. J. White. 2014. The Unintended Effect of Corporate Social Responsibility Performance on Investors' Estimates of Fundamental Value. *Accounting Review* 89 (1): 275-302.

Goffman, E. 1971. *Relations in public*. New York: Harper.

Goldwasser, D. L. 2005. The Past and Future of Reasonable Assurance. *Innovations in Auditing* November: 28-31.

Hamilton, V. L. 1978. Who is responsible? Toward a social psychology of responsibility attribution. *Social Psychology* 41 (4): 316-328.

Hammersley, J. S., L. A. Myers, and C. Shakespeare. 2007. Market reactions to the disclosure of internal control weaknesses and to the characteristics of those weaknesses under section 302 of the Sarbanes Oxley Act of 2002. *Review of Accounting Studies* 13 (1): 141-165.

Heider, F. 1958. *The psychology of interpresonal relations*. New York: Wiley.

Institute of Internal Auditors (IIA). 2008. Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners. Available at https://na.theiia.org/standards-guidance/Public%20Documents/Sarbanes-Oxley_Section_404_--_A_Guide_for_Management_2nd_edition_1_08.pdf.

Kline, R. B. 1998. *Principles and practice of structural equation modeling*. New York: Guilford Press.
Mercer, M. 2005. The fleeting effects of disclosure forthcomingness on management's reporting credibility. *The Accounting Review* 80 (2): 723-744.
Michaels, D. 2014. Hacked Companies Face SEC Scrutiny over Disclosure. *Bloomberg* (July 7).
Ogneva, M., K. R. Subramanyam, and K. Raghunandan. 2007. Internal Control Weakness and Cost of Equity: Evidence from SOX Section 404 Disclosures. *The Accounting Review* 82 (5): 1255-1297.
Palmrose, Z.-V., V. J. Richardson, and S. Scholz. 2004. Determinants of market reactions to restatement announcements. *Journal of Accounting and Economics* 37 (1): 59-89.
Public Company Accounting Oversight Board (PCAOB). 2007. *Auditing Standard No. 5 - An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements*. Washington, D.C.: PCAOB.
Rose, J. M., C. S. Norman, and A. M. Rose. 2010. Perceptions of Investment Risk Associated with Material Control Weakness Pervasiveness and Disclosure Detail. *The Accounting Review* 85 (5): 1787.
Rosenfeld, P., R. A. Giacalone, and C. A. Riordan. 1995. *Impression management in organizations : theory, measurement, practice*. London; New York: Routledge.
Rotter, J. B. 1966. Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs* 80 (1): 1-28.
Schlenker, B. R., T. W. Britt, J. Pennington, R. Murphy, and K. Doherty. 1994. The triangle model of responsibility. *Psychological Review* 101 (4): 632-652.
Schlenker, B. R., B. A. Pontari, and A. N. Christopher. 2001. Excuses and character: Personal and social implications of excuses. *Personality and Social Psychology Review* 5 (1): 15-32.
Schonbach, P. 1990. *Account episodes -- The management or escalation of conflict*. Cambridge: Cambridge University Press.
Scott, M. H., and S. M. Lyman. 1968. Accounts. *American Sociological Review* 33: 46-62.
Securities and Exchange Commission (SEC). 2003. SEC Implements Internal Control Provisions of Sarbanes-Oxley Act; Adopts Investment Company R&D Safe Harbor: Available at http://www.sec.gov/news/press/2003-66.htm.
———. 2005. Staff Statement on Management's Report on Internal Control Over Financial Reporting. Available at http://www.sec.gov/info/accountants/stafficreporting.htm.
———. 2007. Commission Guidance Regarding Management’s Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the ecurities Exchange Act of 1934. Available at http://www.sec.gov/rules/interp/2007/33-8810.pdf.
———. 2014. The Commission's Role in Addressing the Growing Cyber-Threat. Available at http://www.sec.gov/News/PublicStmt/Detail/PublicStmt/1370541287184.
Shaver, K. G., and D. Drown. 1986. On causality, responsibility, and self-blame: A theoretical note. *Journal of Personality and Social Psychology* 50 (4): 697-702.
Snyder, C. R., and R. L. Higgins. 1988. Excuses: Their effective role in the negotiation of reality. *Psychological Bulletin* 104 (1): 23-35.
Summerour, J. 2002. The collusion factor. *Progressive Grocer* 81 (12): 6.
Tyler, J. M., and R. S. Feldman. 2007. The double-edged sword of excuses: When do they help, when do they hurt. *Journal of Social and Clinical Psychology* 26 (6): 659-688.

U.S. House of Representatives. 2002. The Sarbanes-Oxley Act of 2002. In *Public Law 107-204 [H.R. 3763]*. Washington, D.C.: Government Printing Office.
Upton, D. M., and S. Creese. 2012. The Danger from Within. *Harvard Business Review* (September): 94-101.
Verizon. 2015. *2015 Data Breach Investigations Report*. Verizon Inc.
Weiner, B. 1985. An attributional theory of achievement motivation and emotion. *Psychological Review* 92 (4): 548-573.
Wolfe, C. J., E. G. Mauldin, and M. C. Diaz. 2009. Concede or Deny: Do Management Persuasion Tactics Affect Auditor Evaluation of Internal Control Deviations? *The Accounting Review* 84 (6): 2013.
Wood, R. E., and T. R. Mitchell. 1981. Manager behavior in a social context: The impact of impression management on attributions and disciplinary actions. *Organizational Behavior and Human Performance* 28 (3): 356-378.
Yang, H. I. 2012. Capital market consequences of managers' voluntary disclosure styles. *Journal of Accounting & Economics* 53 (1-2): 167-184.

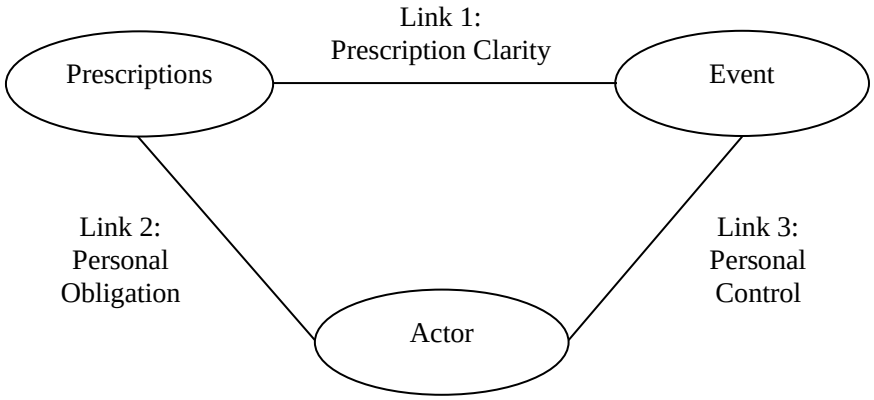
FIGURE 1
The Two-Dimension Framework of Explanations

	Admit the harm	**Not admit the harm**
Admit responsibility	Concession	Justification
Not admit responsibility	Excuse	Denial

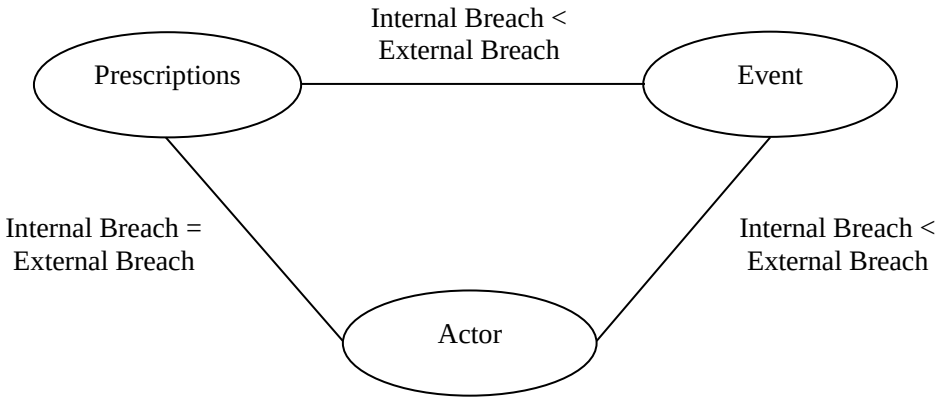
This figure displays a 2 × 2 matrix framework for various types of explanations. The first dimension centers on whether or not the actor admits the harm of an act, and the second consists of whether or not the actor admits responsibility. When both are admitted, the account is a concession, while denial of both constitutes a denial. Admitting responsibility but not harm equates to a justification, and the opposite condition is an excuse.

FIGURE 2
The Triangle Model of Responsibility

Panel A



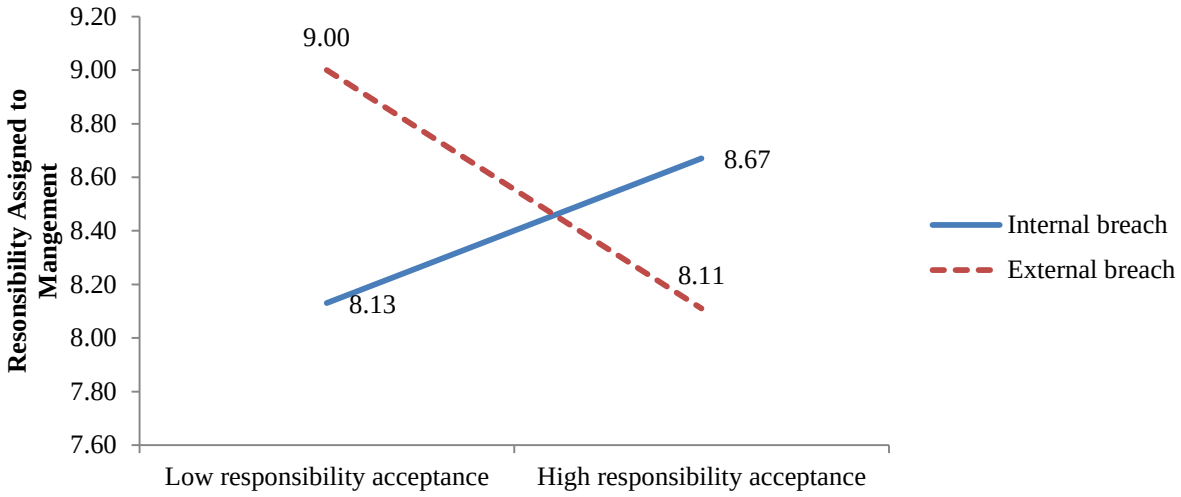
Panel B



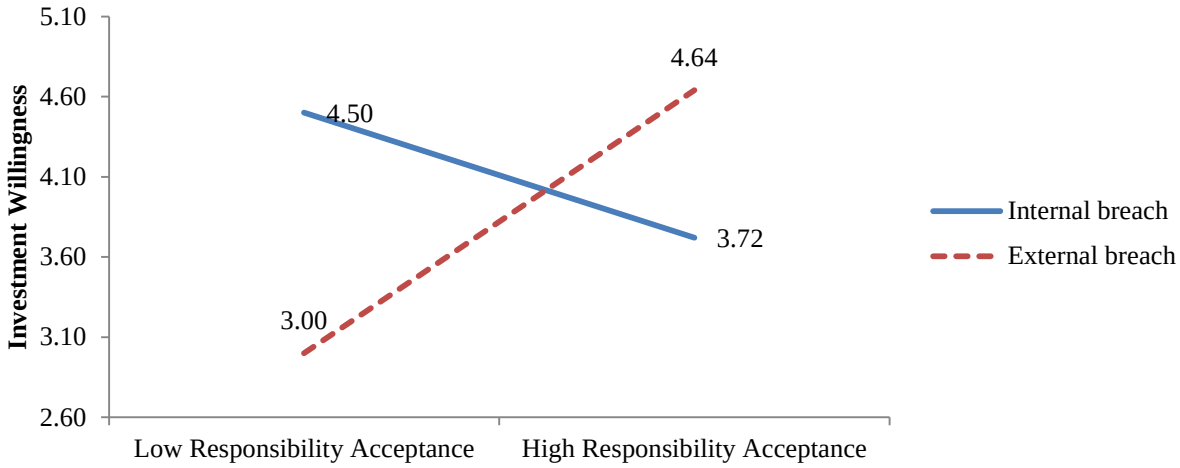
Panel A displays the theoretical constructs and the links between them in the triangle model of responsibility. This model proposes that perceived responsibility is a direct function of the strength of three linkages between the actor, the event, and the relevant prescriptions governing it. People are seen as more responsible when prescriptions governing the event are clear, when they seem to have an obligation to behave in the prescribed ways, and when they are perceived to have personal control over the relevant event.
Panel B displays the predicted strength of each link in the theoretical model. Link 1 and Link 3 are predicted to be stronger in the external breach situation than in the internal breach situation. The strength of Link 2 is predicted to be same in both breach conditions.

FIGURE 3
Interaction Effects of Responsibility Acceptance and Breach in Experiment 1

Panel A: Results on Responsibility Assignment



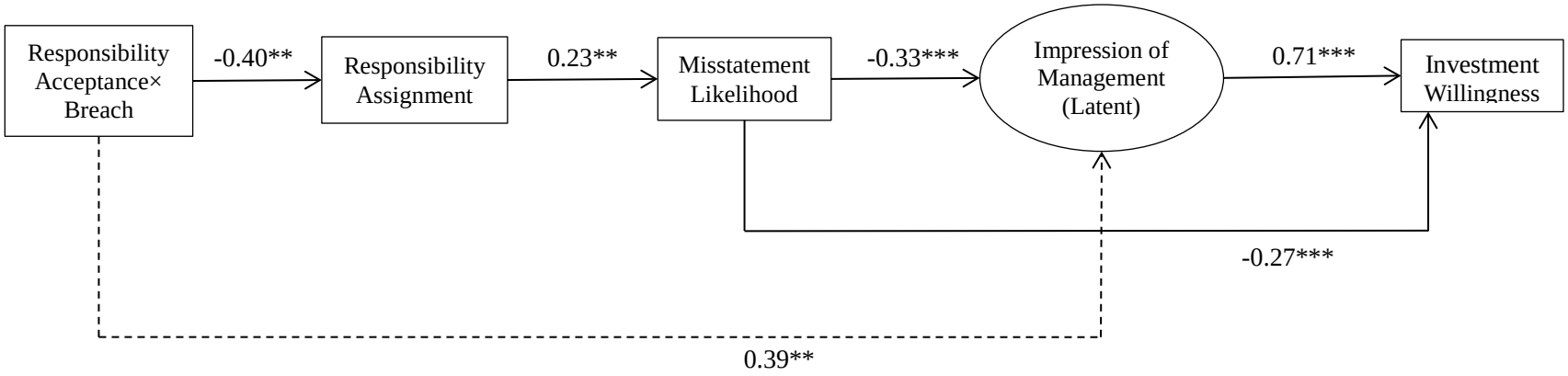
Panel B: Results on Investment Willingness



This figure displays the interaction effects of responsibility acceptance and breach on participants' ratings of responsibility assignment to management (Panel A) and willingness to invest in the firm (Panel B).
Responsibility assignment: responses on an 11-point scale asking participants how much responsibility that they think the management should take for the internal control failure (where 0=no responsibility, and 10=all responsibility).
Investment willingness: a simple average of the responses to two questions: (1) "How willing are you to invest in Griffin's stock?" (where 0 = absolutely not willing to invest, and 10 = absolutely willing to invest), and (2) "Suppose you hold Griffin's stock. How will you change your holdings of Griffin's stock?" (where -5 = significantly decrease, 0 = no change, and 5 = significantly increase).
Breach: in the external (internal) breach condition, the material weakness results from an outsider (a sales representative) hacking into the computer system and changing the sales orders.
Responsibility acceptance: in the high responsibility acceptance condition, the management takes a large proportion of responsibility for the internal control failure; in the low responsibility acceptance condition, the management takes a small proportion of responsibility for the internal control failure.

FIGURE 4

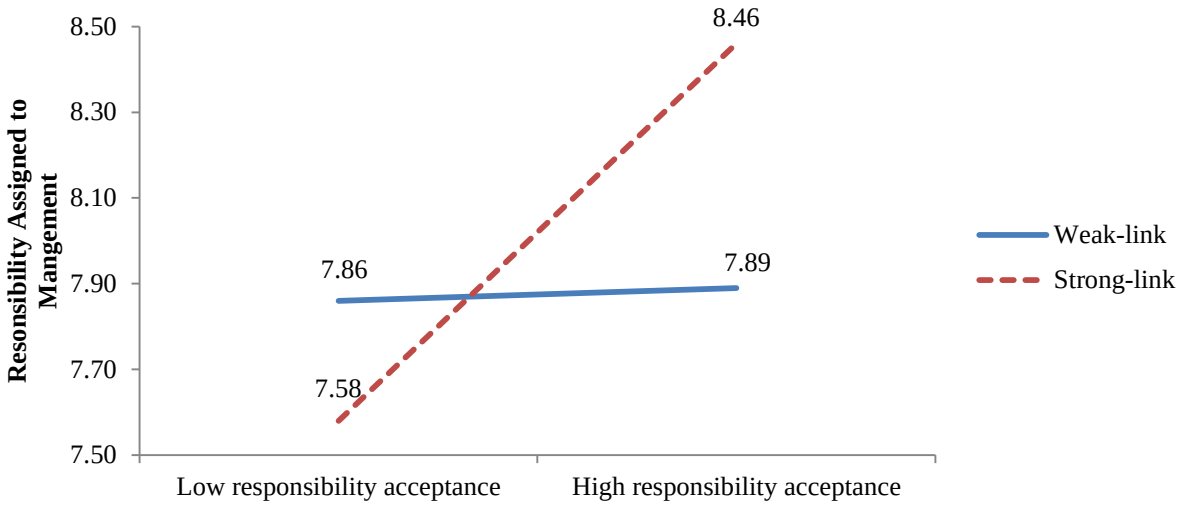
Test of Process



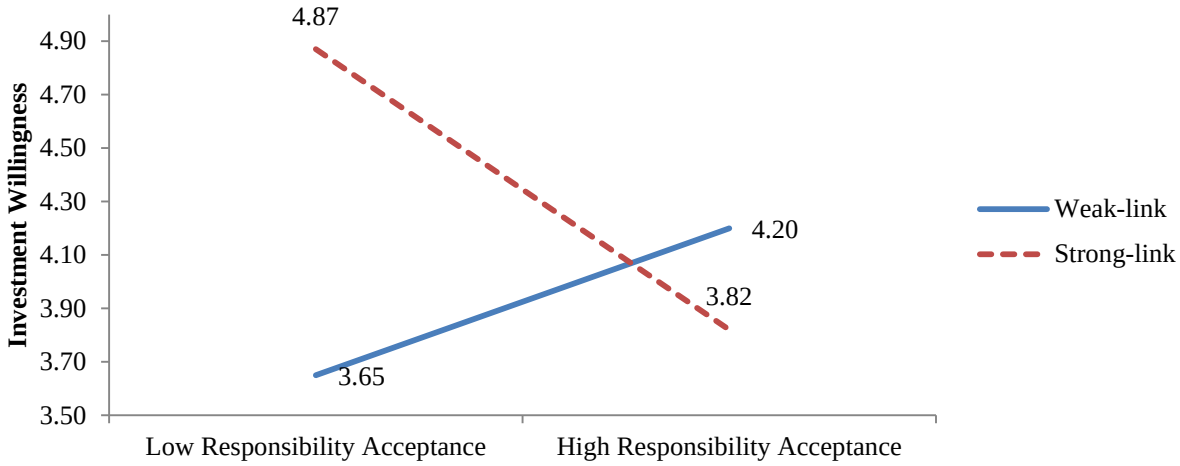
*, **, *** Denotes one-tailed significance at the 10 percent, 5 percent, and 1 percent levels, respectively.
This figure displays the path analysis results using the AMOS software. This model has adequate fit with comparative fit index (CFI) = 0.98 and root mean square error of approximation (RMSEA) = 0.06 (Kline 1998). Standardized coefficients are labelled above the corresponding arrows. Specifically, the interaction term (responsibility acceptance × breach) has a significant direct effect on responsibility assignment (coefficient=-0.40, p=0.03, one-tailed). Responsibility assignment has a significant direct effect on misstatement likelihood (coefficient=0.23, p=0.03, one-tailed). Misstatement likelihood has direct effects on both impression of management (coefficient=-0.33, p<0.01, one-tailed) and investment willingness (coefficient=-0.27, p<0.01, one-tailed). Impression of management has a direct effect on investment willingness (coefficient=0.71, p<0.01, one-tailed). An unexpected link is from the interaction term to impression of management (coefficient =0.39, p=0.04). When modeling the interaction effect of responsibility acceptance and breach, we also estimated the main effects of responsibility acceptance and breach. Refer to Table 3, Panel A for coefficients and significance of each link. Refer to Table 3, Panel B for indirect and total effects of each variable on investment willingness.

FIGURE 5
Interaction Effects of Responsibility Acceptance and Link-Strength in Experiment 2

Panel A: Results on Responsibility Assignment



Panel B: Results on Investment Willingness



This figure displays the interaction effects of responsibility acceptance and link strength on participants' ratings of responsibility assignment to management (Panel A) and willingness to invest in the firm (Panel B).
Responsibility assignment: responses on an 11-point scale asking participants how much responsibility that they think the management should take for the internal control failure (where 0=no responsibility, and 10=all responsibility).
Investment willingness: a simple average of the responses to two questions: (1) "How willing are you to invest in Griffin's stock?" (where 0 = absolutely not willing to invest, and 10 = absolutely willing to invest), and (2) "Suppose you hold Griffin's stock. How will you change your holdings of Griffin's stock?" (where -5 = significantly decrease, 0 = no change, and 5 = significantly increase).
Link Strength: in the strong- (weak-) link condition, a statement emphasizing the chances of an insider hacking is present (absent).
Responsibility acceptance: in the high responsibility acceptance condition, the management takes a large proportion of responsibility for the internal control failure; in the low responsibility acceptance condition, the management takes a small proportion of responsibility for the internal control failure.

TABLE 1
Results on Responsibility Assignment in Experiment 1

Panel A: Descriptive Statistics across Treatment Conditions[a]
Mean (Standard Deviation) *N=Sample Size*

Responsibility Acceptance[c]	Breach[b]		
	Internal	**External**	**Total**
High	8.67 (0.84) *N=18*	8.11 (2.17) *N=18*	8.39 (1.64) *N=36*
Low	8.13 (1.82) *N=16*	9.00 (1.13) *N=15*	8.55 (1.56) *N=31*
Total	8.41 (1.40) *N=34*	8.52 (1.81) *N=33*	8.46 (1.60) *N=67*

Panel B: ANOVA

Sources	Sum of Squares	df	Mean Square	F	*p*-value
Breach (B)	0.425	1	0.425	0.168	0.68
Resp. Acc. (R)	0.502	1	0.502	0.198	0.66
B×R	8.517	1	8.517	3.364	0.03*
Error	159.53	63	2.53		

Panel C: Mean Contrasts

Mean Contrast	Contrast Value	*p*-value
$\mu_{\text{external breach-high}} - \mu_{\text{external breach-low}}$	-0.89	0.06*
$\mu_{\text{internal breach-high}} - \mu_{\text{internal breach-low}}$	0.54	0.17*
$\mu_{\text{external breach-low}} - \mu_{\text{internal breach-low}}$	0.87	0.13
$\mu_{\text{external breach-high}} - \mu_{\text{internal breach-high}}$	-0.56	0.30

[a] Responsibility assignment: responses on an 11-point scale asking participants how much responsibility that they think the management should take for the internal control failure (where 0 = no responsibility, and 10 = all responsibility).
[b] Breach: in the external (internal) breach condition, the material weakness results from an outsider (a sales representative) hacking into the computer system and changing the sales orders.
[c] Responsibility acceptance: in the high responsibility acceptance condition, the management takes a large proportion of responsibility for the internal control failure; in the low responsibility acceptance condition, the management takes a small proportion of responsibility for the internal control failure.
[*] One-tailed equivalent given directional prediction.

TABLE 2
Results on Investment Willingness in Experiment 1

Panel A: Descriptive Statistics across Treatment Conditions[a]
Mean (Standard Deviation) *N=Sample Size*

	Breach[b]		
Responsibility Acceptance[c]	**Internal**	**External**	**Total**
High	3.72 (2.14) *N=18*	4.63 (1.99) *N=18*	4.18 (2.09) *N=36*
Low	4.50 (1.71) *N=16*	3.00 (2.13) *N=15*	3.77 (2.04) *N=31*
Total	4.09 (1.96) *N=34*	3.89 (2.19) *N=33*	3.99 (2.06) *N=67*

Panel B: ANOVA

Sources	**Sum of Squares**	**df**	**Mean Square**	**F**	***p*-value**
Breach (B)	1.42	1	1.42	0.35	0.56
Resp. Acc. (R)	3.09	1	3.09	0.77	0.38
B×R	24.31	1	24.31	6.05	0.01*
Error	253.01	63	4.02		

Panel C: Mean Contrasts

Mean Contrast	**Contrast Value**	***p*-value**
$\mu_{\text{external breach-high}} - \mu_{\text{external breach-low}}$	1.63	0.02*
$\mu_{\text{internal breach-high}} - \mu_{\text{internal breach-low}}$	-0.78	0.13*
$\mu_{\text{external breach-low}} - \mu_{\text{internal breach-low}}$	-1.50	0.04
$\mu_{\text{external breach-high}} - \mu_{\text{internal breach-high}}$	0.91	0.18

[a] Investment willingness: a simple average of the responses to two questions: (1) "How willing are you to invest in Griffin's stock?" (where 0 = absolutely not willing to invest, and 10 = absolutely willing to invest), and (2) "Suppose you hold Griffin's stock. How will you change your holdings of Griffin's stock?" (where -5 = significantly decrease, 0 = no change, and 5 = significantly increase).

[b] Breach: in the external (internal) breach condition, the material weakness results from an outsider (a sales representative) hacking into the computer system and changing the sales orders.

[c] Responsibility acceptance: in the high responsibility acceptance condition, the management takes large proportion of responsibility for the internal control failure; in the low responsibility acceptance condition, the management takes a small proportion of responsibility for the internal control failure.

[*] One-tailed equivalent given directional prediction.

TABLE 3
Test of Process in Experiment 1—Path Analysis

Panel A: Regression Weights (Direct Effects)[a]

			Estimate	Std. Error	*p*-value
Breach (B)	→	Responsibility Assignment	0.28	0.18	0.12
Responsibility Acceptance (R)	→	Responsibility Assignment	0.17	0.17	0.32
B × R	→	Responsibility Assignment	-0.40	0.21	0.03*
Responsibility Assignment	→	Misstatement Likelihood	0.23	0.12	0.03*
Misstatement Likelihood	→	Impression of Management	-0.33	0.11	<0.01*
Breach	→	Impression of Management	-0.14	0.16	0.36
Responsibility Acceptance	→	Impression of Management	-0.33	0.15	0.02
B × R	→	Impression of Management	0.39	0.19	0.04
Impression of Management	→	Investment Willingness	0.71	0.16	<0.01*
Misstatement Likelihood	→	Investment Willingness	-0.27	0.10	<0.01*

Model Fit: *CFI* = 0.98, *RMSEA* = 0.06

Panel B: Effect Coefficients on Investment Willingness

	Direct Effect	Indirect Effect	Total Effect[b]
Breach × Responsibility Acceptance	0.00	0.32	0.32
Responsibility Assignment	0.00	-0.11	-0.11
Misstatement Likelihood	-0.27	-0.23	-0.50
Impression of Management	0.71	0.00	0.71

[a] Misstatement likelihood was measured using an 11-point scale from 0 to 10. Credibility was measured as the average of responses to three questions, each measuring management's competence, honesty, and trustworthiness, respectively. These three questions were measured using 11-point scales from 0 to 10. Affect was measured as the average of responses to four questions, each measuring investors' feelings of happiness, satisfaction, angry, and disappointment, respectively. These four questions were measured using 11-point scales from 0 to 10. Responses to questions on angry and disappointment were reverse-ordered before aggregation.

[b] Total effect is the sum of direct effect and indirect effect (Alwin and Hauser 1975).

[*] One-tailed equivalent given directional prediction.

TABLE 4
Results on Responsibility Assignment in Experiment 2

Panel A: Descriptive Statistics across Treatment Conditions[a]
Mean (Standard Deviation) *N=Sample Size*

	Link Strength[b]		
Responsibility Acceptance[c]	**Weak**	**Strong**	**Total**
High	7.89 (2.02) *N=56*	8.46 (1.22) *N=54*	8.17 (1.70) *N=110*
Low	7.86 (1.52) *N=57*	7.58 (1.99) *N=60*	7.72 (1.78) *N=117*
Total	7.88 (1.78) *N=113*	8.00 (1.72) *N=114*	7.94 (1.75) *N=227*

Panel B: ANOVA

Sources	**Sum of Squares**	**df**	**Mean Square**	**F**	***p*-value**
Link Strength (L)	1.223	1	1.223	0.408	0.52
Resp. Acc. (R)	11.805	1	11.805	3.939	0.05
L×R	10.150	1	10.150	3.387	0.03*
Error	668.244	223	2.997		

Panel C: Mean Contrasts

Mean Contrast	**Contrast Value**	***p*-value**
$\mu_{\text{strong-link/high}} - \mu_{\text{strong-link/low}}$	0.88	<0.01*
$\mu_{\text{weak-link/high}} - \mu_{\text{weak-link/low}}$	0.03	0.92
$\mu_{\text{strong-link/low}} - \mu_{\text{weak-link/low}}$	-0.28	0.39
$\mu_{\text{strong-link/high}} - \mu_{\text{weak-link/high}}$	0.57	0.09

[a] Responsibility assignment: responses on an 11-point scale asking participants how much responsibility they think management should take for the internal control failure (where 0 = no responsibility, and 10 = all responsibility).
[b] Link Strength: in the strong- (weak-) link condition, a statement emphasizing the chances of an insider hacking is present (absent).
[c] Responsibility acceptance: in the high responsibility acceptance condition, management takes a large proportion of responsibility for the internal control failure; in the low responsibility acceptance condition, management takes a small proportion of responsibility for the internal control failure.
* One-tailed equivalent given directional prediction.

TABLE 5
Results on Investment Willingness in Experiment 2

Panel A: Descriptive Statistics across Treatment Conditions[a]
Mean (Standard Deviation) *N=Sample Size*

	Link Strength[b]		
Responsibility Acceptance[c]	**Weak**	**Strong**	**Total**
High	4.20 (2.21) *N=56*	3.82 (2.22) *N=55*	4.01 (2.21) *N=111*
Low	3.65 (2.28) *N=57*	4.87 (2.32) *N=60*	4.27 (2.37) *N=117*
Total	3.92 (2.25) *N=113*	4.37 (2.32) *N=115*	4.14 (2.29) *N=228*

Panel B: ANOVA

Sources	**Sum of Squares**	**df**	**Mean Square**	**F**	***p*-value**
Link Strength (L)	10.027	1	10.027	1.965	0.16
Resp. Acc. (R)	3.576	1	3.576	0.701	0.40
L×R	36.250	1	36.250	7.105	<0.01*
Error	1142.937	224	5.102		

Panel C: Mean Contrasts

Mean Contrast	**Contrast Value**	***p*-value**
$\mu_{\text{strong-link/high}} - \mu_{\text{strong-link/low}}$	-1.05	<0.01*
$\mu_{\text{weak-link/high}} - \mu_{\text{weak-link/low}}$	0.55	0.20
$\mu_{\text{strong-link/low}} - \mu_{\text{weak-link/low}}$	1.22	<0.01
$\mu_{\text{strong-link/high}} - \mu_{\text{weak-link/high}}$	-0.38	0.38

[a] Investment willingness: a simple average of the responses to two questions: (1) "How willing are you to invest in Griffin's stock?" (where 0 = absolutely not willing to invest, and 10 = absolutely willing to invest), and (2) "Suppose you hold Griffin's stock. How will you change your holdings of Griffin's stock?" (where -5 = significantly decrease, 0 = no change, and 5 = significantly increase).

[b] Link Strength: in the strong- (weak-) link condition, a statement emphasizing the chances of an insider hacking is present (absent).

[c] Responsibility acceptance: in the high responsibility acceptance condition, management takes a large proportion of responsibility for the internal control failure; in the low responsibility acceptance condition, management takes a small proportion of responsibility for the internal control failure.

* One-tailed equivalent given directional prediction.

TABLE 6
Archival Tests

Panel A: Descriptive Statistics (n=292)

	Mean	Std. Dev.	Min.	Q1	Median	Q3	Max.
CAR (-2, 2)	-0.003	0.115	-0.416	-0.058	-0.007	0.043	0.600
Locus[a]	0.17	0.379	0.00	0.00	0.00	0.00	1.00
Responsibility Statement	0.95	0.214	0.00	1.00	1.00	1.00	1.00
Non-Strategic Assurance	0.50	0.501	0.00	0.00	1.00	1.00	1.00
Strategic Assurance	0.28	0.451	0.00	0.00	0.00	1.00	1.00
Remediation	0.74	0.439	0.00	0.00	1.00	1.00	1.00
Consequence	0.46	0.769	0.00	0.00	0.00	1.00	2.00
No. of weakness	1.99	1.650	1.00	1.00	1.00	3.00	17.00
BIG4	0.32	0.466	0.00	0.00	0.00	1.00	1.00
Market Value	4.672	1.738	0.67	3.574	4.515	5.610	10.30
Book/Market ratio	-0.228	17.511	-291.90	0.338	0.758	1.334	6.89
Loss	0.54	0.499	0.00	0.00	1.00	1.00	1.00
Earnings Coinciding	0.38	0.486	0.00	0.00	0.00	1.00	1.00
CAR (-1, 1)	-0.001	0.102	-0.414	-0.047	-0.006	0.038	0.725

Panel B: Correlation Matrix (Pearson/Spearman above/below the diagonal; n=292)

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)
1. CAR (-2, 2)		-0.062	-0.066	-0.044	**0.156**	0.033	0.013	0.000	-0.001	-0.008	-0.003	-0.001	0.011
2. Locus	-0.075		0.018	0.017	0.041	0.061	*-0.115*	-0.020	-0.014	0.077	0.030	0.040	0.056
3. Responsibility Statement	-0.044	0.018		**0.224**	0.035	-0.023	0.051	-0.050	**0.118**	-0.033	-0.015	**0.116**	0.076
4. Non-Strategic Assurance	-0.020	0.017	**0.224**		**-0.630**	0.062	**0.125**	0.010	**0.147**	0.045	0.044	0.076	-0.057
5. Strategic Assurance	*0.110*	0.041	0.035	**-0.630**		0.045	**-0.149**	*0.101*	**-0.133**	*-0.103*	0.048	-0.018	-0.004
6. Remediation	0.019	0.061	-0.023	0.062	0.045		-0.030	**0.133**	-0.048	0.043	**0.117**	0.051	0.093
7. Consequence	0.093	**-0.133**	0.045	**0.125**	**-0.151**	-0.023		**-0.177**	**0.173**	**0.185**	0.011	-0.038	*-0.111*
8. No. of weakness	-0.093	-0.025	-0.066	-0.033	**0.139**	**0.155**	**-0.244**		0.053	0.033	-.030	-0.064	0.095
9. BIG4	0.024	-0.014	**0.118**	**0.147**	**-0.133**	-0.048	**0.170**	-0.015		**0.597**	0.038	-0.051	**-0.185**
10. Market Value	0.008	0.080	-0.023	0.032	*-0.107*	0.049	**0.165**	0.015	**0.604**		**0.130**	**-0.306**	**-0.203**
11. Book/Market ratio	0.054	0.088	-0.014	0.036	0.028	0.085	0.014	-0.047	-0.028	**-0.244**		-0.062	-0.094

12. Loss	-0.044	0.040	**0.116**	0.076	-0.018	0.051	-0.043	-0.056	-0.051	**-0.278**	0.045		0.053
13. Earnings Coinciding	-0.028	0.056	0.076	-0.057	-0.004	0.093	*-0.097*	0.086	**-0.185**	**-0.204**	*-0.100*	0.053	

Panel C: Regression results

$$Market\ returns = \beta_0 + \beta_1 Locus + \beta_2 Responsibility\ statement + \beta_3 NonStrategic\ assurance + \beta_4 Strategic\ assurance + \beta_5 Controls$$

DV: CAR (-2, 2)	Coefficient	t	Sig.
(Constant)	0.015	0.35	0.724
Locus	-0.022	-1.17	0.243
Responsibility Statement	-0.063	-1.83	0.069
Non-Strategic Assurance	0.032	1.63	0.105
Strategic Assurance	0.067	3.16	0.002
Remediation	0.014	0.81	0.417
Consequence	0.008	0.80	0.423
No. of weakness	-0.003	-0.66	0.511
BIG4	0.009	0.46	0.649
Market Value	-0.001	-0.15	0.880
Book/Market ratio	0.000	-0.40	0.690
Loss	-0.003	-0.21	0.832
Earnings Coinciding	0.013	0.87	0.387
Adj. R^2	1.0%		

[a] The locus variable excluded 15 observations that do not mention the factors related to the weakness.
In Panel B, a **bold** (*italics*) style indicates two-tailed p-value ≤0.05 (≤0.10).

Appendix A: Examples of Each Category in the Archival Coding

Variable	Level	Example
Locus	Internal	"…the Company did not maintain effective internal control over financial reporting, solely relating to improper segregation of duties identified **within the Company's Defense segment**. During the fourth quarter of 2011, **members of the Company's financial staff** had access to automated accounting functions and the ability to administer security over the processing of accounting data." *(National Presto Industries, Inc., 10-K filing for the fiscal year ended December 31, 2011)*
	External	"…the Company did not maintain effective controls over the preparation and review of the income tax provision. Management's review of the income tax provision, which was prepared by an **outside tax advisor**, failed to identify an error related to the nature and timing of temporary differences related to indefinite lived intangible assets when establishing a valuation allowance on deferred tax assets." *(Affirmative Insurance Holdings, Inc., 10-K filing for the fiscal year ended December 31, 2009)*
Responsibility Statement	Present	"The Company's management is responsible for establishing and maintaining adequate internal control over financial reporting." *(First Potomac Realty Trust, 10-K filing for the fiscal year ended December 31, 2010)*
	Absent	Absence of such (or similar) statement *(e.g., Subay, Inc., 10-K filing for the fiscal year ended September 30, 2010)*
Reasonable Assurance Argument	Non-Strategic	"Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies and procedures may deteriorate." *(Telestone Technologies Corporation, 10-K filing for the fiscal year ended December 31, 2011)*
	Strategic	"Based on that evaluation, our Chief Executive Officer and our Chief Financial Officer concluded that the current disclosure controls and procedures as of December 31, 2010 were not effective… Our management does not expect that our disclosure controls or our internal controls will prevent all errors and all fraud. A control system, no matter how well conceived and operated, can provide only reasonable rather than absolute assurance that the objectives of the control system are met… Because of the inherent limitations in all control systems, no evaluation of controls can provide absolute assurance that all control issues and instances of fraud (if any) within the Company have been detected." *(Applied Minerals Inc., SEC 10-K filling for the fiscal year ended December 31, 2010)*
	Absent	Absence of the "reasonable assurance" argument *(e.g., Zale Corporation, SEC 10-K filling for the fiscal year ended July 31, 2010)*

Appendix B: Manipulations in Experiment 2

Manipulation of Prescription:

[Strong-link] **An authoritative computer security report recently warned companies against being complacent about their internal control systems as these can be easily circumvented by insiders, and advised companies to implement measures to guard against the possibility of hacking by their own employees.**

[Weak-link] *(The above paragraph is absent.)*

Manipulation of Responsibility Acceptance:

There was a failure to maintain adequate access controls over the sales recording system. Because of this access control weakness in the control system, the Company's sales recording system was breached. A sales representative was able to successfully hack into the computerized sales recording system, change the sales orders, and steal customers' data.

[High responsibility acceptance] **A control system should be well conceived and operated to provide reasonable (not absolute) assurance that the objectives of the control system are met.**
Our management team acknowledges the responsibility to ensure that our control system should provide reasonable assurance that control issues (including this hacking instance) will be detected.

[Low responsibility acceptance] **A control system, no matter how well conceived and operated, can provide only reasonable rather than absolute assurance that the objectives of the control system are met.**
Our management team is of the opinion that no control system can provide absolute assurance that all control issues (including this hacking instance) will be detected.

Management will be taking further remediation efforts during the next fiscal year. The independent auditor has also conducted its own evaluation of Griffin's internal control over financial reporting, and identified the same control weakness.