'Breaching' Auditor Judgments of Information Security Effectiveness

Research-in-Progress

K. Asli Basoglu
University of Delaware
Newark, DE
asli@udel.edu

John D'Arcy
University of Delaware
Newark, DE
jdarcy@udel.edu

Abstract

In this in-progress study we explore whether aspects of a prior data security breach, along with prior audit performance, work to decrease auditor objectivity of information security (InfoSec) weaknesses in the subsequent audit period. We use SOX Section 404 as the contextual setting and our analysis is based on a unique dataset from publicly available sources. Preliminary results suggest that not only does former audit performance influence auditor judgments of InfoSec performance, but also the strength of this relationship changes based on public attention. We found no evidence for the influence of past breach severity on auditors' judgments nor did we find that the influence of public attention is direct. Instead, it appears that auditors can be lured toward decreased objectivity in an indirect manner, based on the weight of public attention that increases their desire to validate past audit evaluations. Implications and plans for future research are discussed.

Keywords: Information Security, SOX 404, Data Breach, Audit Performance

Introduction

The importance of information security (InfoSec) in general and firms' internal InfoSec practices in particular has increased in recent years due to the growing number of data security breaches experienced by organizations. Research indicates that the average cost of a data breach to organizations is over 3 million U.S. dollars per incident, with substantial higher costs for more severe breaches (in terms of total records lost) (Ponemon Institute 2013). Equally damaging are the reputational costs that accrue from the increased (presumably negative) media coverage and public attention that follow the public announcement of a data breach incident. In one recent survey, 86% of respondents indicated that they would cease doing business with a company that had a data breach.[1]

To address the financial and reputational damage caused by data security breaches, and the problem of compromises to InfoSec in general, federal and state governments have enacted regulations and standards that mandate organizations' internal InfoSec practices. For instance, evolving data breach notification laws and other security-based regulations (e.g., Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA)), have imposed new encryption rules for transmitting data and authentication procedures for accessing corporate systems. In the current study, we focus on one such law that affects all publicly traded companies in the U.S – the Sarbanes-Oxley Act (SOX) of 2002. SOX was enacted in reaction to several high-profile corporate accounting scandals (e.g., Arthur Anderson, Enron, WorldCom) in an effort to restore public trust in capital markets. Per the requirements of SOX Section 404 (hereafter SOX 404), top management must certify the accuracy of the company's financial reports and the effectiveness of the internal controls

[1] http://www.semafone.com/86-customers-shun-brands-following-data-breach/

around the financial reporting (Rice et al. 2013). Given that modern accounting and financial reporting systems are heavily dependent on information technology, adhering to the requirements of SOX 404 falls largely on the InfoSec function within the organization (Warner 2005). One way to consider this relationship is that an insecure system would not be considered a source of reliable financial information due to the possibility of unauthorized transactions or manipulation of numbers. Hence, the requirements of SOX 404 include internal controls related to information technology, software, and security/access issues surrounding a company's financial reporting.

The "teeth" behind SOX 404 is that an outside auditor firm must attest to, and report on, management's assessment of its internal controls over financial reporting. For the portions of SOX 404 that pertain to InfoSec, the outside audit essentially provides an independent and presumably unbiased measure of a firm's internal InfoSec performance. This assessment is a critical aspect of SOX 404, as any identified weaknesses (or auditors' failure to report such weaknesses) in internal InfoSec policies, procedures, and technologies can carry considerable negative consequences such as regulatory and market-based penalties (Rice et al. 2013).

Although auditors are required by law to maintain independence and professional skepticism, research suggests that available information can dilute their judgments and raise questions about their accountability (Glover 1997). On this point, certain negative organizational events (e.g., misstatement in a financial report, internal fraud) have been shown to heighten auditors' level of sensitivity (e.g., Lobo and Zhao 2013) and downwardly bias their judgments of internal control effectiveness (Kaplan 1985). The rationale is that such negative events are a signal of a firm's internal control weaknesses, which heighten auditors' sensitivity toward the audit, and increase the likelihood of overzealous findings. Given that auditors are known to pursue a risk-averse approach throughout their audits, former negative events may initiate negative hypothesis framing and force them to seek evidence that will confirm their expectations. Further, auditors may not act completely objective as their perceptions about the firm may have already been formed in the former audit periods. The purpose of the current study is to explore these phenomena in the context of InfoSec and SOX 404 compliance. We consider a data security breach as a highly consequential negative organizational event and focus on two aspects of breaches – breach severity and public attention associated with the breach – and explore whether these factors, along with prior audit performance, work to unduly influence auditor judgments of InfoSec performance in the following year. Our preliminary analysis revealed some interesting findings. As opposed to objective measures (i.e., severity of breach), subjective factors (i.e., public attention) seem to drive auditor judgments of InfoSec performance along with former audit performance. We aim to further explore this "social influence" angle of auditor judgment as this research progresses.

Conceptual Rationale and Hypotheses Development

In considering the factors that might promote decreased auditor objectively toward the InfoSec aspects of SOX 404, we draw from the social psychology literature. Regulatory focus theory (Higgins 1997) distinguishes between two major categories of goals: (i) promotion goals, and (ii) prevention goals. A promotion goal focuses on the acquisition of aspirations, heightens one's sensitivity to positive outcomes (their presence or absence), is associated with a risky bias (i.e., a tendency to undertake actions), and leads to an inclination to approach strategy; that is, to pursue all means of advancement. A prevention goal, in contrast, focuses on the satisfaction of duties and obligations, heightens one's sensitivity to negative outcomes, is associated with a conservative bias (i.e., a tendency to undertake actions), and leads to an avoidance strategy; that is, to carefully avoid any mistakes.

The prevention category aligns with the goals of auditors. Auditors are trained to be sensitive to evidence that reduces the risk of failing to detect material errors or weaknesses in their clients' financial statements. The accounting literature refers to this behavior as professional skepticism or conservative behavior (Smith and Kida 1991). Therefore, auditors try to prevent making any mistakes by analyzing all possible signals that may potentially have a negative consequence. In the context of our study, prior data security breaches may signal the presence of weaknesses in InfoSec processes to auditors, and thereby prime them to look for future InfoSec weaknesses in a more scrutinized manner. This priming effect can be problematic to the integrity of the audit because not all data security breaches can be directly linked to InfoSec weaknesses, or prior InfoSec weaknesses that were exposed from a past data breach may have been rectified and no longer exist in the following year's audit period.

Although there is emerging evidence that the occasional data breach is viewed as a normal cost of doing business, at least in the minds of investors (Gordon et al. 2011), there is tremendous variation in the scope and severity of data breaches. To give a recent example, Target's high-profile breach of credit card data affected an estimated 40 million customers and cost the company over $61 million U.S. dollars in expenses[2]. We conjecture that once such a severe data breach becomes public knowledge, it will permeate into the minds of auditors, perhaps even subconsciously, and influence their evaluations of that firm's InfoSec performance. The rationale here is that auditors' conservative biases will kick in and their sensitivity toward negative information will become amplified, resulting in more InfoSec weaknesses being pointed out during the audit process. The end result is decreased auditor objectivity.

Theoretical support for this position comes from social psychological research on attention. In particular, attention research suggests that if something is novel or unusual for its category, it will garner a disproportionate amount of scrutiny (Jones and McGillis 1976). We apply similar reasoning in our study and purport that a more severe data breach – in terms of records affected - will stand out relative to other more common data breaches and attract the attention of auditors, potentially biasing their future evaluation of the firm's InfoSec performance. Empirical findings provide some evidence to support this assertion. For instance, research on corporate wrongdoings suggests that the greater the scale of wrongdoing event (e.g., auto recall, industrial accident), the greater the public attention and the stronger social disapproval (Carroll 2009). Similarly, Da et al. (2011) found that certain attention-grabbing stocks have a strong influence on investors' overall investment strategies. In the InfoSec context, Wang et al. (2008) found that the more intense and prevalent a network security attack (e.g., Melissa virus), the more the public attention it garners and the more the ordinary users scrutinize their InfoSec practices.

In summary, even though auditors pursue an objective evaluation during the audit process, we propose that the severity of a past data security breach sends a signal regarding the quality of a firm's current internal InfoSec efforts, resulting in increased auditor scrutiny and thereby influencing the auditors' evaluation of current period InfoSec performance. Central to our argumentation (and a necessary condition to test our hypothesis, which we have validated in our data) is that no additional data breaches have occurred for the firm under investigation during the current audit period. That is, the firm had a data breach of varying severity in the period prior to the audit, but none in the current audit period (i.e., the year following the breach). We also acknowledge extant research that found a strong relationship between past audit performance and auditor evaluations in the subsequent year (e.g., Rice and Weber 2012). Auditors' opinions are shaped by their relationship with the firm being evaluated and the former evaluations that the audit firm provided to that organization. Accordingly, we expect pre-breach audit evaluations (year t-1) to influence post-breach evaluations (year t+1) and control for this in our hypothesizing. This leads to the following:

H1: Controlling for the previous year's audit performance, severity of the data security breach (at year t=0) will negatively influence the next year's audit performance.

We also consider public attention associated with a prior data security breach as a factor that can decrease auditor objectivity of future internal InfoSec performance. In particular, public attention surrounding a breach can sensitize an auditor to the firm's InfoSec practices and lead to more scrutinized future evaluations. This is similar to our earlier reasoning regarding the influence of breach severity. As stated by Zavyalova et al. (2012), "when a firm or its peers engage in wrongdoing, the media and stakeholders actively seek new information about the firm and recalibrate their impressions of it" (p. 1082). Indeed, research on corporate wrongdoing and other damaging organizational incidents has found that negative media coverage (which is a precursor to and strong correlate of public attention) induces individuals' scrutiny of the firm and can result in a more negative evaluation (Carroll 2009; Rindova et al. 2005).

Organizational scholars studying reputation offer some explanation for this process. This work posits that reputation is a valuable resource in that it reduces the uncertainty that stakeholders face in evaluating firms as potential suppliers of needed products and service (Rindova et al. 2005). In this sense, reputation acts a signal that enables stakeholders to assess relevant firm attributes (Zavyalova et al. 2012). To the extent that reputation is reflecting in the public attentiveness toward a firm, or the public attentiveness toward a particular issue involving the firm, it can assist stakeholders in evaluating a firm's competency

[2] http://money.cnn.com/2014/03/14/news/companies/target-breach/

regarding the particular area of interest (Rindova et al. 2005). We apply this same reasoning to the current study and conjecture that public attention following a data security breach helps reduce auditors' uncertainty of the firm's InfoSec performance and this evaluation carries over to the subsequent audit period; and further, considering that this public attention is in response to a negative event, the increased public attention will resonate with auditors in a negative sense and push them, perhaps very slightly and even subconsciously, toward a more negative evaluation of the firm's InfoSec performance. There is some evidence of this phenomenon in practice, as it was empirically demonstrated that auditors behaved more conservatively when faced with media attention following the high-profile corporate scandals involving Enron and WorldCom (Feldmann and Read 2010; Geiger et al. 2005).

We can also argue for the influence of a prior data breach's public attention on subsequent auditor judgments from a cognitive workload perspective. Public attention following an organizational incident provides a ready-made evaluation of the organization that reduces the need for stakeholders to evaluate the organization's attributes and qualities directly (Rindova et al. 2005; Zavyalova et al. 2012). Applying this view to our study, public attention associated with a data security breach provides a "quick and dirty" evaluation of the affected organization's InfoSec practices, at least to some extent. Again, and perhaps subconsciously in an attempt to reduce their cognitive load, auditors may be affected by this public attention such that it reduces the need for a completely objective evaluation of the firm's InfoSec practices in the subsequent audit period. As with H1, we argue that this relationship will exist over and above the influences of the prior year's audit performance. This leads to the following hypothesis:

H2: Controlling for the previous year's audit performance, public attention associated with the data security breach (at year t=0) will negatively influence the next year's audit performance.

As previously stated, extant research provides a strong link between auditors' judgments in prior periods and those reported in subsequent periods. Rice and Weber (2012) reason that this is due to the additional scrutiny and effort that auditors apply to firms with a history of accounting and control problems. Hence, a negative audit evaluation (i.e., identification of an internal control weakness) is a salient event for the audit firm and will likely remain in their consciousness for future engagements with the firm being audited. Alternatively, should a new audit firm be employed, past audit performance can serve as a point of reference. Past audit performance therefore provides a baseline for future audit evaluations. We propose that in the InfoSec context, this baseline can be influenced by the two aspects of data security breaches described above – severity and public attention – and we describe our reasoning as follows.

Following several high-profile corporate scandals (e.g., Arthur Anderson, Enron, WorldCom), the integrity of the audit profession fell into question and public attention became an important factor in auditor evaluations (Geiger et al. 2005). We therefore conjecture that with stronger public attention associated with a data security breach, auditors may feel more pressure to reinstate their credibility which may push them to revert back to the firm's prior audit (i.e., the baseline) as a means of additional scrutiny. The rationale here is that in response to strong public attention, auditors are likely to use the former audit as a "safe harbor" to justify the validity and credibility of their former opinion, or in cases in which they did not conduct the former audit, the validity and credibility of the audit profession in general. Thus, auditors will be less likely to deviate from the prior audit in the form of a completely new and objective audit when there is strong public attention given to the firm's earlier InfoSec performance. We can apply the same reasoning when considering breach severity and argue that this characteristic of a data breach will serve to amplify the influence of prior audit performance on subsequent auditor judgment. Statistically speaking, these purported relationships support an interactive influence of both public attention and breach severity on prior audit performance, such that the influence of prior audit performance is stronger when (i) the public attention of the breach is increased and (ii) the severity of a breach is increased. Although somewhat speculative at this point, we offer the following hypotheses:

H3: Previous year's audit performance will have a stronger positive influence on the next year's audit performance as the public attention associated with a data security breach (at year t=0) is increased.

H4: Previous year's audit performance will have a stronger positive influence on the next year's audit performance as the severity of the data security breach (at year t=0) is increased.

Methodology and Data Analysis

To conduct the preliminary data analysis presented in this paper, we constructed a dataset from publicly available sources. First, we conducted a detailed search for data security breaches for the period 2005-2012 using the privacyrights.org website. We limited our search to breaches of publicly-traded companies due to the nature of our study – i.e., audit performance. Privacyrights.org includes a chronology of publicly available data security breaches starting from 2005 along with detailed descriptions of the breaches, including the number of records impacted by the breach. We used this as our measure of breach severity (Severity). Note that we only included data security breaches of publicly-traded companies through 2012 because the audit data (which we describe below) is only available through the end of 2013, and we utilize audit data for the year (four quarters) following each breach as part of our analysis. For each company in our sample, we obtained its CIK code, which is used by the U.S. Security and Exchange Commission to uniquely identify each company for its audit filings. This was necessary to match the breached companies with the audit data described below. Our breach sample consisted of 558 total breaches, across 373 different companies (i.e., 373 different CIK codes).

The second source of data is disclosures of internal control weaknesses obtained from the Audit Analytics database. Audit Analytics contains detailed audit information on over 1,200 accounting firms and 15,000 publicly traded companies starting from the year 2000. We initially focused on internal control weaknesses with reason codes 22 and 52, which are both described as disclosures of information technology, software, security, and access issues. Both categories pertain to ineffective SOX 404 internal controls. During our initial analysis, we found that none of the companies in our sample had internal control weaknesses with code 22 over the audit timeframe of our study (2004-2013); hence, our measure of audit performance consists of internal control weaknesses with reason code 52 only.

Audit Analytics codes internal control weaknesses as "1" or "0" for each quarter to signify whether or not auditors reported any weaknesses in that time period. Hence, we cannot determine whether the "1" signifies the existence of only one or multiple InfoSec weaknesses. For each of the data security breaches in our sample, we summed the total reason code 52 weaknesses for the (i) four quarters preceding the breach and (ii) the four quarter following the breach. To give an example, if the breach occurred on March 17, 2005, we summed the total 52 reason code weaknesses from quarters 1 through 4 of 2004 as the measure of prior audit performance (Prior_Audit) and the total 52 reason code weaknesses from quarter 2 of 2005 through quarter 1 of 2006 as the subsequent year's audit performance (Next_Audit). We followed this same procedure for every data security breach in our sample. For reasons unbeknownst to us, Audit Analytics did not provide audit data for many of the companies for the timeframes under investigation in our study. Hence, the total number of breaches for which we had complete reason code 52 audit performance data for the four quarters preceding and the four quarter following each breach was 242. We used this as our final sample.

The third source of data is Internet search activity, using Google Insights for Search. Using Google Insights, users can examine search trends over various periods for specific metropolitan areas, with daily search data available when examining search volume over a period of three months or less. Google provides search volume results on a scale of 0 to 100 by dividing the total search volume at each point in time by the highest value within that same time frame; hence, the results are normalized and not estimates of absolute search volume (see https://support.google.com/trends/answer/4365533?hl=en).

Ripberger (2011) provides a strong case for Internet search trends as a valid indicator of public attention. In particular, he found strong convergent validity between Google search volume and media-based public attention (e.g., articles appearing in The New York Times) and offers the logic that Internet search activity encompasses an individual's thought, willingness, and effort to search on a particular topic. Given that Google is the most widely used Internet search engine by far (Da et al. 2011), we deemed it an appropriate mechanism to gauge public attention associated with the data security breaches in our study.

For each of the 242 data breaches in our sample, we collected daily search volume on the company that had been breached for the three months prior to and following the publicly announced breach date (as noted, three months is the extent to which Google provides daily search volume; longer periods are provided in weekly or monthly terms). Our search term for each company was the company name that appeared in the public breach announcement provided by privacyrights.org. In some cases we had to provide a slightly modified company name (e.g., PepsiCo vs. Pepsi) to obtain the Google search results.

To construct our measure of public attention (Pub_Att), we followed the logic of event studies that measure stock market reactions to significant corporate events (e.g., corporate wrongdoings, computer virus infestations) and developed a baseline level of Google search volume activity for each company for the three months prior to its breach. This is akin to stock market-based event studies that first develop an estimation period prior to the event as a means to ascertain abnormal returns (Brown and Warner 1985). We then took the average of the Google search volume results for the three days immediately following the breach announcement and subtracted that value from the baseline Google search volume value. Our choice of three days following the breach as the "event window" is consistent with extant event studies in the accounting and finance literature.

We tested our hypotheses with OLS regression. Since we had moderating hypotheses, we standardized all variables to account for possible multicollinearity between the main effects and interaction effects (Aiken and West 1991). Note that we ran separate models with interaction terms (one model with the main effects and Prior_Audit*Public_Att and one model with the main effects and Prior_Audit*Severity) so as not to obviate their independent influences (Aiken and West 1991). Table 1 shows our regression results.

Table 1. Regression Analysis

	Model 1 (R^2 = .22)			Model 2 (R^2 = .18)		
DV: Next_Audit	**Std. Beta**	**t-value**	**p-value**	**Std. Beta**	**t-value**	**p-value**
Prior_Audit	0.590	4.199	**0.000**	1.039	1.974	**0.052**
Pub_Att	0.091	0.844	0.402	0.073	0.670	0.505
Severity	0.126	1.184	0.240	0.199	1.584	0.118
Prior_Audit*Pub_Att	0.276	1.99	**0.050**			
Prior_Audit*Severity				0.684	1.252	0.215

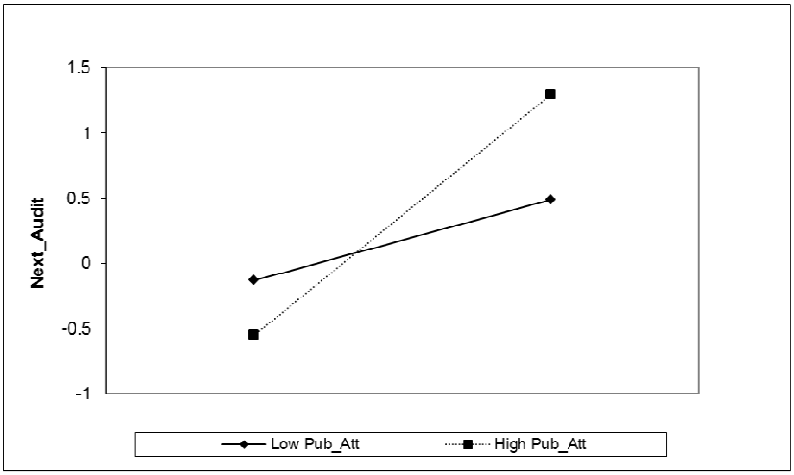

Figure 1: Moderating Effect of Public Attention

As expected, our preliminary results support a strong positive relationship between prior audit performance (Prior_Audit) and the subsequent year's audit performance (Next_Audit). The results do not support H1 or H2 in that neither breach severity (Severity) nor public attention associated with the breach (Pub_Att) had a significant relationship with the subsequent year's audit (Next_Audit). Moreover, there is no support for H4 in that the proposed interaction between prior audit and breach severity (Prior_Audit*Severity) was not statistically demonstrated. Interestingly, the results indicate a significant interaction between prior audit and public attention (Prior_Audit*Pub_Att), thereby supporting H3. To interpret this relationship in more detail, we provide the interaction graph in Figure 1. The solid line represents one standard deviation below the mean on Pub_Att and dotted line represents one standard deviation above the mean on Pub_Att. The interaction graph demonstrates that the relationship between

prior audit and the following year's audit is stronger (i.e., steeper slope) for breaches that garnered higher public attention compared to those that received lower public attention.

Discussion, Implications, and Future Plans

Our preliminary results suggest that not only does former audit performance influence auditor judgments of InfoSec performance, but also the strength of this relationship changes based on public attention. Contrary to our expectations, we found no evidence for the influence of past breach severity on auditors' judgments nor did we find that the influence of public attention is direct. Instead, it appears that auditors can be lured toward decreased objectively in an indirect manner, based on the weight of public attention that increases their desire to validate past audit evaluations. In finding that an objective characteristic of the data breach (i.e., severity) is not as influential in distorting auditors' judgments of InfoSec performance, it appears that perception is stronger than reality in terms of the potential factors that decrease auditor objectivity.

We recognize that our explanations are largely speculative at this point and that alternative explanations cannot be ruled out. Our future work will dig deeper into the area of InfoSec audit using case studies and interviews of auditors and the InfoSec managers that meet with auditors. We will also attempt to validate the findings presented here using more robust statistical analyses that consider potential endogeneity issues and investigates the influences of variables such as auditor tenure, firm size, profitability, type of security breach (e.g., internal vs. external; intentional vs. accidental), etc. One potential avenue is to construct a larger panel-style dataset that includes a control set of similar firms that did not experience a data security breach (see Kwon et al. 2013 for a similar example). In addition to enhancing our dataset and conducting improved statistical analyses, we plan to build a more tenable theoretical foundation for the factors that lead to decreased auditor objectivity in the InfoSec context.

Finally, the current research extends knowledge of the impact of data security breaches beyond the organizational-level and firm-specific factors that have been considered in prior work. We offer changes in individual cognition, in this case in terms of auditor judgment, as an additional outcome of data security breaches. From a methodological perspective, our work provides an alternative to the vast body of InfoSec literature that relies on cross-sectional surveys. Notably, by using auditor evaluations of InfoSec weaknesses (i.e., reason code 52), which were obtained from Audit Analytics, we provide one of the few third-party measures of InfoSec performance.

References

Aiken, L.S., and West, S.G. 1991. "*Multiple Regression: Testing and Interpreting Interactions*," Thousand Oaks, CA: Sage.

Brown, S.J., and Warner, J.B. 1985. "Using Daily Stock Returns: The Case of Event Studies," *Journal of Financial Economics*, 14, pp. 3-31.

Carroll, C.E. 2009. "The Relationship between Firms' Media Favorability and Public Esteem," *Public Relations Journal*, (3:4), pp. 1-32.

Da, Z., Engelberg, J., and Gao, P. 2011. "In Search of Attention," *The Journal of Finance*, (66:5). Pp. 1461-1499.

Feldman, D. A., and Read, W.J. 2010. "Auditor Conservatism after Enron," *AUDITING: A Journal of Practice & Theory*, (29:1), pp. 267-278.

Geiger, M. A., Raghunandan, K., and Rama, D.V. 2005. "Recent Changes in the Association Between Bankruptcies and Prior Audit Opinions," *Auditing: A Journal of Practice & Theory,* (24:1), pp. 21–35.

Glover, S. 1997. "The Influence of Accountability and Time Pressure on Auditor Judgment Processing of Nondiagnostic Information," *Journal of Accounting Research*, (35:2), pp. 213-226.

Gordon, L.A., Loeb, M.P., and Zhou, L. 2011. "The Impact of Information Security Breaches: Has there been a Downward Shift in Costs?" *Journal of Computer Security*, 19, pp. 33-56.

Higgins, E. T. 1997. "Beyond pleasure and pain," *American Psychologist, 52*, 1280-1300.

Jones, E.E., and McGillis, D. 1976. "Correspondent Inferences and the Attribution Cube: A Comparative Reappraisal," in *New Directions in Attribution Research, Volume 1*, J.H. Ickes and R.F. Kidd (eds.), Hillsdale, NJ: Erlbaum, pp. 389-420.

Kaplan S. E. 1985. "The Effect of Combining Compliance and Substantive Tasks on Auditor Consensus," *Journal of Accounting Research,* 23, pp. 871-77.

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

Lobo, G., and Zhao, Y. 2013. "Relation between Audit Effort and Financial Report Misstatements: Evidence from Quarterly and Annual Restatements," *The Accounting Review*, (88:4), pp. 1385-1412.

Ponemon Institute. 2013. *2013 Cost of Data Breach Study: Global Analysis*. Traverse City, MI: Ponemon Institute, LLC.

Rice, S.C., and Weber, D.P. 2012. "How Effective is Internal Control Reporting under SOX 404? Determinants of the (Non-) Disclosure of Existing Material Weaknesses," *Journal of Accounting Research*, (50:3), pp. 811-843.

Rice, S.C., Weber, D.P., and Wu, B. 2013. "Does SOX 404 Have Teeth? Consequences of the Failure to Report Existing Internal Control Weaknesses," Working Paper, Available at SSRN: http://ssrn.com/abstract=2239965 or http://dx.doi.org/10.2139/ssrn.2239965

Rindova, V.P., Williamson, I.O., Petkova, A.P., and Sever, J.M. 2005. "Being Good or Being Known: An Empirical Examination of the Dimensions, Antecedents, and Consequences of Organizational Reputation," *Academy of Management Journal*, (48:6), pp. 1033-1049.

Ripberger, J.T. 2011. "Capturing Curiosity: Using Internet Search Trends to Measure Public Attentiveness," *Policy Studies Journal*, (39:2), pp. 239-259.

Smith, J.F., and Kida, T. 1991. "Heuristics and Biases: Expertise and Task Realism in Auditing," *Psychological Bulletin*, (109:3), pp. 472-489.

Wang, J., Xiao, N., and Rao, H.R. 2008. "Drivers of Information Security Search Behavior: An Investigation of Network Attacks and Vulnerability Disclosures," *ACM Transactions on Management Information Systems*, (1:1), pp. 1-23.

Warner, R. 2005. *Information Security and Section 404 of the Sarbanes-Oxley Act*. Bethesda, MD: SANS Institute.

Zavyalova, A., Pfarrer, M.D., Reger, R.K., and Shapiro, D.L. 2012. "Managing the Message: The Effects of Firm Actions and Industry Spillovers on Media Coverage Following Wrongdoing," *Academy of Management Journal*, (55:5), pp. 1079-1101.