Article

Not peer-reviewed version

Do Auditors Consider Cybersecurity Insurance in Pricing Audits?

Angel Arturo Pacheco-Paredes , Elizabeth Hendrix Turner * , Clark M Wheatley

Posted Date: 26 January 2026

doi: 10.20944/preprints202601.1813.v1

Keywords: breach risk; audit fees; corporate governance; cybersecurity; cyber insurance

 doi:10.20944/preprints202601.1813.v1

Article

Do Auditors Consider Cybersecurity Insurance in Pricing Audits?

Angel Arturo Pacheco-Paredes [1], Elizabeth Hendrix Turner [2,*] and Clark M Wheatley [3]

[1] A. R. Sanchez Jr. School of Business, International Banking and Finance Studies, Texas A&M International University, Laredo, TX, USA

[2] Augusta University, USA

[3] Florida International University, USA

* Correspondence: diaturner@augusta.edu

Abstract

Prior research has shown that security breaches are associated with an increase in auditor fees (Smith, Higgs, and Pinsker, 2019). Auditors serve an important role in external governance with respect to a firm's overall risk management protocol. Cybersecurity insurance provides financial protection against unexpected security breaches, helping businesses manage risk that could otherwise lead to significant financial hardship. Our study examines the role cybersecurity insurance plays in mitigating the breach risk audit fee premium. Using a sample of firms from 2008-2018, we explore how auditors view audit risk related to breach risk and whether cybersecurity insurance mitigates this risk premium. Our evidence suggests that the purchase of cyber insurance results in higher audit fees, but that coupling cyber risk oversight within the audit committee with the acquisition of cyber insurance reduces auditors' perceptions of risk in post breach periods. These results should provide guidance to firms and regulators as they seek to address and mitigate the business risks associated with information technology.

Keywords: breach risk; audit fees; corporate governance; cybersecurity; cyber insurance

1. Introduction

Gründl, Guxha, Kartasheva, and Schmeiser (2021, p. 868) characterize cybersecurity risk as a "low frequency/high severity" risk, while Gazert, Schmit and Kolb (2016) note that cybersecurity insurance has typically been bundled with coverage for crisis management costs. Recent research has found that firms with higher cybersecurity risk are more likely to implement cyber risk management and that, for banks and insurers, this is seen by investors and impounded into (increased) firm value (Gatzert and Schubert, 2022). This leads us to question whether this perceived reduction in business risk is also reflected in how auditors price firms' audits. Gatzert and Schubert (2022 p. 727) note that "despite its costs, risk management can be valuable if it contributes to the reduction of profit volatility," but what if some of the costs of that risk management can be offset by savings elsewhere?

A number of recent investigations have examined the determinants of audit pricing with respect to income smoothing (Chang, Ho, Liu, and Quyang 2021), corporate social responsibility (Du, Xu, and Yu 2020), and the types of equity compensation paid to audit committee members (Shrader and Sun 2019) among others. We expand this line of inquiry further, by investigating whether an association exists between the mitigation of client business risk and audit fees. Specifically, do auditors factor client cybersecurity insurance into the pricing of audits.

The increase in data breach incidents around the world has raised concerns about how organizations can protect proprietary information and maintain the integrity of databases. The existence of cybersecurity risk requires that managers decide on the type of risk profile they are comfortable with. According to Mukhopadhyay, et al. (2013 p.11) Cyber-risk is defined as "the risk involved with a malicious electronic event that causes disruption of business and monetary loss." In

 doi:10.20944/preprints202601.1813.v1

response, risk management systems aim to assess risks and take steps to reduce risk to an acceptable level (Guttman and Roback, 1995). The primary generic framework for risk management in the U.S. comes from the Committee of Sponsoring Organizations of the Treadway Commission [COSO]. Since 2004 COSO has placed an emphasis on promoting Enterprise Risk Management [ERM]. In September 2017, COSO issued the 2017 COSO ERM Framework, entitled *Enterprise Risk Management–Integrating with Strategy and Performance*. Even though this framework does not target cyber risk specifically, it can aid organizations in assessing and managing cyber risk.

The risk of data breach incidents has become more complex and more common in today's interconnected business environment. For example, on September 7, 2017, Equifax reported a cybersecurity incident where consumer records from a number of databases were stolen. The primarily information stolen included names, Social Security numbers, birth dates, addresses and, in some instances, the driver's license numbers of 143 million U.S. consumers. On July 23, 2019 Equifax agreed to pay up to $700 million to settle with the Federal Trade Commission. To Date, this settlement is the largest for a data breach incident.

Risk management can be decomposed into two primary activities: risk assessment and risk mitigation (Guttman and Roback, 1995). In the assessment of risk, managers identify risks based on the organization's infrastructure. Once threats and risks are identified, managers can ignore, mitigate, transfer, or retain the risk (Vacca, 2012). Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management. Even when businesses try to control risk by investing in cybersecurity measures and systems, some risk remains, referred to as residual risks. Organizations may transfer risk, by purchasing specialized insurance. Indeed, Shackelford (2012) argues that the best approach in addressing cyber risk is to address the problem technologically where possible, and to buy insurance for those things you cannot control (such as residual risk) because insurance provides the organization with financial security against risk and uncertainty by helping it to reduce the potential for financial loss (Mukhopadhyay et al. 2013).

The expected loss from association with a risky client increases the auditor's business risk. Studies have shown that audit firms consider business risk in pricing audits (Brumfield, Elliott, and Jacobson 1983; Bell, Landsman, and Shackelford 2001) and that audit firms charge higher audit fees to firms involved in controversial activities (Lyon and Maher 2005; Koh and Tong 2013). Biener, Eling, and Wirfs (2015) show, however, that the distribution of cyber risk differs significantly from the distribution of other types of operational risk and Smith, Higgs, and Pinsker (2018) find evidence that breaches are associated with increases in audit fees. Other than fees, "…public accounting firms have a simple strategy to reduce their legal losses. By avoiding engagements with clients likely to fail or otherwise fall from grace with the capital markets" (Sellers, Fogerty, and Jadallah 2020). In this study we extend prior research by investigating the association between cybersecurity liability and audit fees. This study also contributes to the literature on the usefulness of disclosing material cybersecurity risks, specifically related with insurance coverage. Third, this study contributes to the disclosure literature by inspecting whether the voluntary disclosure of insurance, mitigates the incidence of breaches in future periods. Lastly, we explore the effect of audit committees that charge their members with specific oversight duties on privacy and data security risk, on audit fees.

2. Literature Review and Hypothesis Development

Today one of the fastest growing threats to any organization is cyber risk. The *Risk Based Security* report notes that the year 2018 had the second highest number or breaches and exposed records ever, with 6,515 breaches and over 5 billion records exposed. Clearly, the increase in the number of cyber incidents and its impact on companies is a concern for managers. According to the annual *Cost of a Data Breach Report* by the Ponemon Institute and IBM (2019) the average total cost of a data breach in the U.S. has grown from $3.54 million in 2006 to $8.19 million in 2019. Studies have shown that cyber incidents can also invoke other threats such as business interruption, and reputation and brand damage (Allianz 2015; Camillo 2017 and Xie, Lee and Eling 2019).

 doi:10.20944/preprints202601.1813.v1

Prior studies have explored the effect of cyber-attacks on a variety of issues. Ettredge and Richardson (2003) use a sample of internet firms subject to hacker attacks and find a negative market reaction to those firms when compared to similar firms that were not attacked. Cavusoglu, Mishra, and Raghunathan (2004) and Kannan, Rees, and Sridhar (2007) find that the announcement of an Internet security breach is negatively associated with firm value. A recent paper by Amir, Levi, and Livne (2018) find a severe negative market reaction to undisclosed cyber-attacks and a small negative effect for disclosed cyber-attacks. Indeed, studies have demonstrated a negative market reaction to cyber incidents when these events are revealed.

There has been considerable interest from the public related to companies' protection of customer data, and several states in the U.S. have passed laws that regulate data protection. The state of California, for example, made six amendments to the California Consumer Privacy Act on October 13, 2019. In spirit, those amendments will regulate how businesses retain and use electronic consumer data and will provide the authority to penalize companies for data breaches. Prior to the amendments, the law required only that companies disclose any breach that might impact California residents.

In 2005 the Securities and Exchange Commission (SEC) required that most public companies disclose risk factors annually (SEC 2005). On February 21, 2018 the SEC released guidance on public disclosure requirements on cybersecurity risk. According to this guidance, "companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity" (pages 6-7). In addition, the guidance recommends that companies disclose the costs associated with maintaining cybersecurity protections (insurance coverage, payments for services, and etc.) (SEC 2018).

A number of studies have explored the disclosure of cybersecurity activities (Gordon, Loeb, Lucyshyn, and Sohail 2006; Wang, Kannan, and Ulmer 2013; Campbell et al. 2014; Li, No, and Wang 2018). Gordon et al. (2006) find that after Sarbanes-Oxley, there is an increase in voluntary disclosure of information security activities. Contrary to the belief that risk factor disclosures are boilerplate, Campbell et al. (2014) find that managers' risk factor disclosures provide useful information that investors incorporate into firm valuation. Furthermore, managers disclose more risk factors and dedicate a greater portion of their disclosures to these factors when risks are higher and more significant. More recently, Li et al. (2018) find that cybersecurity risk disclosures are not boilerplate. The SEC's 2018 disclosure rule has, however, also lead to an increase in firms' cybersecurity risk disclosures regardless of the degree of cybersecurity risk.

Since companies are not immune to cyber risks, businesses might use cyber insurance to mitigate potential losses. Such coverage is not a new. Majuca, Yurcik, and Kesan (2006) mark 1998 as the year when cyber insurance was first introduced. Today cyber insurance products have become more complex due to the increase in regulation and more sophisticated threats. At the high end, these products cover claims arising from internet content, internet security, technology errors, and omissions (Mukhopadhyay et al. 2013).

The purchase of cyber insurance provides risk mitigation for companies. According to Kesan, Majuca, and Yurcik (2005) firms that have recently acquired cyber insurance have identified the transfer of risk, monitoring, fast action against threats, and protection against hacking as advantages of cyber insurance products. Cyber insurance policies may also include first-party and third-party exposure. The first party covers against data destruction, theft, hacking, and extortion. The third-party insurance provides coverage for business that are responsible for clients' online security against errors or omissions that arise out of the professional service. According to *Aon's U.S. Cyber Market Update* (2019), there are a total of 184 insurers that reported cyber insurance premiums in 2017 and, in 2018, cyber insurance premiums totaled over $2 billion.[1]

[1] The market is, however, concentrated in three insurers: American International Group (AIG), Chubb, and XL Group that together have a market share of over 45%.

 doi:10.20944/preprints202601.1813.v1

Smith et al. (2018) examine whether auditors consider breach risk in their assessment of business risk. Their results show that breaches are associated with an increase in audit fees. In addition, they find evidence that the presence of board-level risk committees mitigates the breach risk and audit fee premium. This leads us to question whether auditors adjust their business risk assessments when client firms purchase cyber insurance products. Although we expect a relation between cyber insurance and audit fees, the direction of that relation is not clear. For instance, Li et al. (2018) document that the disclosure of cyber risk factors is related to future reported cybersecurity incidents. The voluntary disclosure of the purchase of cyber insurance could thus be indicative of a firm's increased risk and be associated with higher audit fees.

On the other hand, Biener et al. (2015, p.145) note that insurers demand assessments of cyber risk prior to offering coverage and these assessments "may have positive and valuable side-effects in that it may increase company awareness of cyber risk, potentially increasing self-protective efforts." Indeed, Majuca et al. (2006) conclude that cyber insurance can result in higher security investment by increasing the level of safety for information technology (IT) infrastructure, thus the disclosure of cyber insurance and its risk mitigation could be associated with lower audit fees. Given the above, our first hypothesis regarding an association between cyber insurance and audit fees is non-directional. Similarly, since the auditor, by examining transactions, will be aware of any cyber insurance whether it has been publicly disclosed or not, any association with audit fees will not be dependent on disclosure prior to a breach. Thus, our second hypothesis predicts that any association of audit fees with cyber insurance will not be dependent on disclosure prior to a breach. In null form these hypotheses are:

H1: *The disclosure of cyber insurance is not associated with audit fees.*

H2: *The disclosure of existing cyber insurance after a reported cybersecurity incident is not associated with audit fees.*

While the purchase of cyber insurance may be associated with a higher risk profile, it might also convey a company's commitment to cybersecurity (Majuca et al. 2006, Biener et al. 2015). As a result, firms that purchase cyber insurance may or may not be subject to more cybersecurity incidents in the future. Thus, our third hypothesis is also non-directional.

H3: *The purchase of cyber insurance is not associated with the likelihood of subsequently reported cybersecurity incidents.*

A growing number of companies are revising their audit committee charters to reflect the audit committee's cybersecurity oversight responsibilities. According to KPMG's 2015 Global Audit Committee Survey 43% of companies assign the greatest responsibility for cybersecurity risk to the audit committee. Higgs et al. (2016) find that the existence of a technology committee mitigates the negative abnormal stock return associated with a breach, and Smith, et al. (2018) find that when firms audit committees are more active around the report of a breach the firms experience lower audit fees. This leads us to propose the following hypothesis:

H4: *Audit committee charter provisions regarding cybersecurity oversight will be associated with lower audit fees.*

3. Method

3.1. Sample

Our sample period covers the period 2008-2018. We obtain the sample from the intersection of the *Audit Analytics* and *Compustat* databases. Table 1 presents the sample selection process. We

 doi:10.20944/preprints202601.1813.v1

exclude 11,558 firm-years with missing audit fee and audit opinion data, and 706 firms-years missing data required to estimate our regression models. This results in a total sample of 61,227 firms-years.

Table 1. Sample Selection Process.

Active-firm year observations with non-missing price and assets from COMPUSTAT (2008-2018)	73,491
Less firm-year observations:	
Missing audit fee and audit opinion data	11,558
Missing financial data variables	706
Firm year observation for full sample analysis	61,227
Less firms year observations:	
Excluded by propensity score matching procedure	59,141
Firms-year observation for matched analysis	2,086

We identify our sample of firms that disclose the purchase of cybersecurity insurance from *Thomson-Reuters Eikon, annual, interim, proxy & information, SEC U.S. registrations and press documents*. We used the following keywords in our search: "*Cyber Security Liability*" and "*Cyber Security Insurance*." This procedure yields a sample of 400 unique firms, with the first disclosure made on December 12, 2008 and the last on December 30, 2018. Merging the firms with insurance disclosure with our full sample yields 341 unique firms (1,043 firm year observations) that have indicated the presence of a cyber insurance policy. Table 2 presents the sample distribution of first-time disclosures. The increase in the number of firms disclosing the presence of a cyber insurance policy for the first time could be explained by the new SEC disclosure requirements on cybersecurity risk.

Table 2. First Time Sample Firms Disclosing Cyber Security Insurance by Year.

Year	Unique Firms Identified	Unique Firms Without Missing Data
2008	2	2
2009	1	1
2010	2	2
2011	14	12
2012	15	13
2013	22	18
2014	41	40
2015	52	45
2016	77	63
2017	69	55
2018	105	90
Total Firms	400	341

3.2. Models

We include determinants of audit fees identified in prior literature. We control for financial condition, audit complexity, audit risk, and financial distress. We use the natural log of total assets (*LNASSETS*) as a proxy for firm size to control for firm characteristics. We include Zmijewski's (1984) financial distress score (*DISTRESS*), the ratio of current assets to current liabilities (*CR*), an indicator variable set equal to 1 if the firm had negative operating income (*LOSS*), the return-on-assets (*ROA*), and the ratio of long-term debt to total assets (*LEVERAGE)* to control for financial condition.

To account for audit complexity, we include the square root of number of segments (*SEGMENTS*), an indicator variable set equal to 1 if the firm reported foreign earnings (*FOREIGN*), and book value of equity divided by market value of equity (*BTM*). To control for the impact of auditor expertise we include auditor specialist (*SPECIALIST*). We also include an indicator variable set to 1 if the company has a fiscal year-end in December (*YE*). We include an indicator variable set

 doi:10.20944/preprints202601.1813.v1

to 1 if the auditor is among the Big 4 (*BIG4*), and an indicator set to 1 if the company changed auditors during the year (*CHANGE*).

We also include variables to account for audit risk factors: the natural log of the number of days from the end of the fiscal year to the audit report date (*DELAY)*, an indicator variable set to 1 if the firm reported a restatement (*RESTATE*), an indicator variable set to 1 if the company's internal controls were found to be inadequate (*IC*), and an indicator variable set to 1 if the audit opinion includes a going concern modification (*GC*). To control for inherent risk, we use the ratio formed by the sum of inventory and receivables divided by total assets (*INVREC*).

We investigate the association between cybersecurity insurance and audit fees by estimating the following:

$$\begin{aligned} LNAUDITFEES = {} & \beta_0 + \beta_1 CYBER\_INSURANCE_{it} + \beta_2 TECHNOLOGY_{it} + \beta_3 RISK_{it} \\ & + \beta_4 COMPLIANCE_{it} + \beta_5 BREACH_{it-1} + \beta_6 LNASSETS_{it} + \beta_7 DISTRESS_{it} \\ & + \beta_8 INVRECV_{it} + \beta_9 LEVERAGE + \beta_{10} ROA_{it} + \beta_{11} SEGMENTS_{it} + \beta_{13} GC_{it} \\ & + \beta_{13} LOSS_{it} + \beta_{14} FOREIGN_{it} + \beta_{15} YE_{it} + \beta_{16} CHANGE_{it} + \beta_{17} BIG4_{it} + \beta_{18} IC_{it} \\ & + \beta_{19} SPECIALIST_{it} + \beta_{20} CR_{it} + \beta_{21} BTM_{it} + \beta_{22} RESTATE_{it} + \beta_{23} DELAY_{it} + \varepsilon_{it} \end{aligned} \quad (1)$$

where:

LNAUDITFEES: is the natural log of audit fees;

CYBER_INSURANCE: is set equal to 1 if the firm discloses the presence of a cyber-insurance policy in fiscal year t, and 0 otherwise;

RISK: is set equal to 1 if the company discloses the presence of a "Risk" committee in their proxy statement for the current year, and 0 otherwise;

TECHNOLOGY: is set equal to 1 if the company discloses the presence of a "Technology" committee in their proxy statement for the current year, and 0 otherwise;

COMPLIANCE: is set equal to 1 if the company discloses the presence of a "Compliance" committee in their proxy statement for the current year, and 0 otherwise;

BREACH: is set equal to 1 if the company announces a breach disclosed on privacyrights.org during the last fiscal year, and 0 otherwise;

AUDIT_CYBER_OVERSIGHT: is set equal to 1 if the company's audit committee charter provides a provision regarding cybersecurity oversight, and 0 otherwise;

LNASSETS: is the natural log of total assets;

DISTRESS: Zmijewski's (1984) financial distress score;

RESTATE: is set equal to 1 if the firm reports a restatement during the current year, and 0 otherwise;

INVRECV: is the ratio of receivables and inventory to total assets;

LEVERAGE: is the ratio of long-term debt to total assets;

ROA: is the ratio of earnings before interest and taxes to total assets;

SEGMENTS: is the square root of the number of business segments;

GC: is set equal to 1 if the firm received a going concern audit report during the current year, and 0 otherwise;

LOSS: is set equal to 1 if the firm reports negative income before extraordinary items, and 0 otherwise;

FOREIGN: is set equal to 1 if the firm reports foreign earnings, and 0 otherwise;

YE: is set equal to 1 if the firm uses calendar year-end reporting, and 0 otherwise;

CHANGE: is set equal to 1 if the firm changed auditors during the year, and 0 otherwise;

BIG4: is set equal to 1 if the auditor is a Big 4 auditor, and 0 otherwise;

IC: is set equal to 1 if the company's internal controls were found to be inadequate, and 0 otherwise;

SPECIALIST: is the sum of the square root of the total assets of the clients of an auditor in a specific industry divided by the total sum of the square root of the total assets of all clients of the auditor;

CR: is the ratio of current assets to current liabilities;

 doi:10.20944/preprints202601.1813.v1

BTM: is the book value of equity divided by market value of equity; and

DELAY: is the natural log of the number of days from the fiscal year-end to the audit report date.

$BREACH_{t-1}$: is set equal to 1 if the company announces a breach disclosed on privacyrights.org in the previous fiscal year, and 0 otherwise;

We add interaction terms to the model to test for differences between the pre and post breach periods (H2). If disclosing the presence of a cyber-insurance policy results in a decrease in audit fees, we expect the coefficient on the interaction term to be negative (*CYBER_INSURANCE * POST_BREACH*).

POST_BREACH: is equal to 1 if the firm observation is after a data breach, 0 otherwise;

CYBER_INSURANCE * POST_BREACH; is the interaction of *CYBER_INSURANCE* and *POST_BREACH.*

$$\begin{aligned} LNAUDITFEES = {} & \delta_0 + \delta_1 CYBER\_INSURANCE_{it} + \delta_2 POST\_BREACH_{it} \\ & + \delta_3 CYBER\_INSURANCE * POST\_BREACH_{it} + \delta_4 TECHNOLOGY_{it} + \delta_5 RISK_{it} \\ & + \delta_6 COMPLIANCE_{it} + \delta_7 BREACH_{it-1} + \delta_8 LNASSETS_{it} + \delta_9 DISTRESS_{it} \\ & + \delta_{10} INVRECV_{it} + \delta_{11} LEVERAGE + \delta_{12} ROA_{it} + \delta_{13} SEGMENTS_{it} + \delta_{14} GC_{it} \\ & + \delta_{15} LOSS_{it} + \delta_{16} FOREIGN_{it} + \delta_{17} YE_{it} + \delta_{18} CHANGE_{it} + \delta_{19} BIG4_{it} + \delta_{20} IC_{it} \\ & + \delta_{21} SPECIALIST_{it} + \delta_{22} CR_{it} + \delta_{23} BTM_{it} + \delta_{24} RESTATE_{it} + \delta_{25} DELAY_{it} \\ & + \delta_{25} LAMBDA_{it} + \varepsilon_{it} \end{aligned} \quad (2)$$

To test H3, we employ a logit model to predict whether the presence of cyber insurance reduces the likelihood that a firm experiences a data breach. Our test model is:

$$\begin{aligned} BREACH_{t+1} = {} & \alpha_0 + \alpha_1 CYBER\_INSURANCE_{it} + \alpha_2 TECHNOLOGY_{it} + \alpha_3 RISK_{it} \\ & + \alpha_4 COMPLIANCE_{it} + \alpha_5 BREACH_{it-1} + \alpha_6 LNASSETS_{it} + \alpha_7 LOSS_{it} \\ & + \alpha_8 LEVERAGE + \alpha_9 INTANGIBLES_{it} + \alpha_{10} SEGMENTS_{it} + \varepsilon_{it} \end{aligned} \quad (3)$$

$BREACH_{t+1}$: is set equal to 1 if the company announces a breach disclosed on privacyrights.org in the next fiscal year, and 0 otherwise;

MERGER: is set equal to 1 if the company is involved in merger activity in the fiscal year t, and 0 otherwise;

GROWTH: is the one-year growth rate in sales in fiscal year t.

The disclosure of the purchase of a cyber insurance policy represents a selection made by the organization, therefor self-selection bias may be a concern in this study. To address this concern, we follow the Heckman (1979) two-stage approach. To determine the cyber insurance prediction model, we employ a model similar to that in Higgs et al. (2016) and Smith, Higgs, and Pinsker (2018). The model is related to the likelihood of a firm reporting a data breach, which would likely increase the probability a firm would purchase cyber-insurance. The cyber insurance prediction model is:

$$\begin{aligned} & Prob(CYBER\_INSURANCE = 1) \\ & = \gamma_0 + \gamma_1 INTANGIBLES_{it} + \gamma_2 TECHNOLOGY_{it} + \gamma_3 RISK_{it} + \gamma_4 COMPLIANCE_{it} \\ & + \gamma_5 BREACH_{\mathrm{it}-1} + +\gamma_6 LNASSETS_{it} + \gamma_7 DISTRESS_{it} + \gamma_8 INVRECV_{it} \\ & + \gamma_9 LEVERAGE + \gamma_{10} ROA_{it} + \gamma_{11} SEGMENTS_{it} + \gamma_{12} GC_{it} + \gamma_{13} LOSS_{it} \\ & + \gamma_{14} FOREIGN_{it} + \gamma_{15} YE_{it} + \gamma_{16} CHANGE_{it} + \gamma_{17} BIG4_{it} + \gamma_{18} IC_{it} \\ & + \gamma_{19} SPECIALIST_{it} + \gamma_{20} CR_{it} + \gamma_{21} BTM_{it} + \gamma_{22} RESTATE_{it} + \gamma_{23} DELAY_{it} + \varepsilon_{it} \end{aligned} \quad (4)$$

where:

INTANGIBLES: is the natural log of (1+ total intangible assets), measured at the beginning of the year.

Since the Heckman selection model requires the identification of an exogenous independent variable, we follow Smith et al. (2018) and use the natural log of 1 plus total intangible assets (*INTANGIBLES*) in the first-stage model. We exclude this variable from the second-stage model and include a vector of the same control variables included in Equation (1).

We also conduct propensity score matching to control for observation differences between firms with and without cyber insurance. We obtain the predicted probabilities from the first stage logistic

 doi:10.20944/preprints202601.1813.v1

model from Equation (4). We match one-to-one without replacement. This results in 1,043 matched pairs (2,086 total observations). The comparison of variable means for the matched pairs is presented in Table 7.

To test H4 we use equation 2 and include the *AUDITCOMMITTEECYBEROVER* variable. This variable is an indicator variable which equals 1 for those instances where the charter of the audit committee includes cybersecurity oversight duties.

4. Results

Table 3 provides descriptive statistics for the key variables used in the audit fee test. All variables are winsorized at the 1st and 99th percentiles. The mean (median) audit fee for the sample is $2,200,000 ($730,000). Approximately 2 percent of the firms make a cyber-insurance policy disclosure (*CYBER_INSURANCE*). On average 0.5 percent of our sample firms experience a data breach incident (*BREACH*). The mean (median) size is 5.99 (6.33). Of the total sample, 5 percent of the firms have a risk committee (*RISK*). We find that 40.4 percent of the firm year observations report losses (*LOSS*). We also observe that 61 percent of the firm year observations are audited by Big 4 accounting firms (*BIG4*). Overall, about 11% of the sample reported a going concern (*GC*) opinion. The average book to market ratio is 0.414.

Table 3. Descriptive Statistics.

Variable	Mean	SD	Q1	Median	Q3
AUDITFEES	2,200,000	5,400,000	210,000	730,000	1,900,000
LNAUDITFEES	13.389	1.595	12.278	13.499	14.445
CYBER_INSURANCE	0.017	0.129	0.000	0.000	0.000
BREACH	0.005	0.072	0.000	0.000	0.000
INTANGIBLES	3.075	2.846	0.000	2.700	5.465
TECHNOLOGY	0.023	0.151	0.000	0.000	0.000
RISK	0.051	0.220	0.000	0.000	0.000
COMPLIANCE	0.027	0.163	0.000	0.000	0.000
LNASSETS	5.999	2.955	4.292	6.332	7.968
DISTRESS	-2.752	17.751	-4.309	-3.279	-1.762
INVRECV	0.253	0.237	0.056	0.184	0.389
LEVERAGE	0.188	0.252	0.000	0.092	0.297
ROA	-0.107	0.433	-0.057	0.029	0.086
SEGMENTS	1.750	1.145	1.000	1.732	2.449
GC	0.119	0.324	0.000	0.000	0.000
LOSS	0.404	0.491	0.000	0.000	1.000
FOREIGN	0.312	0.463	0.000	0.000	1.000
YE	0.767	0.423	1.000	1.000	1.000
CHANGE	0.080	0.271	0.000	0.000	0.000
BIG4	0.612	0.487	0.000	1.000	1.000
IC	0.027	0.161	0.000	0.000	0.000
SPECIALIST	0.123	0.251	0.003	0.014	0.092
CR	2.379	3.585	0.295	1.436	2.727
BTM	0.414	0.481	0.136	0.348	0.636
RESTATE	0.083	0.276	0.000	0.000	0.000
DELAY	4.248	0.347	4.043	4.234	4.454
LAMBDA	3.084	0.828	2.448	3.048	3.653

Table 4 reports the correlation coefficients for the variables used in the main model. We note that *LNAUDITFEES* is correlated with *CYBER_INSURANCE* suggesting a positive relation. This correlation provides univariate support for the auditor increasing fees in response to the disclosure of cybersecurity insurance in the current year. We note that three of the independent variables

 doi:10.20944/preprints202601.1813.v1

(*INTANGIBLES*, *LNASSETS*, and *BIG4*) are highly correlated (correlation > 0.5) with *LNAUDITFEES*, indicating possible collinearity issues. It is not unexpected that the size of a firm (LNASSETS) is correlated with higher audit fees. It is also not surprising that hiring a BIG4 is correlated with higher audit fees. Given that intangibles are often hard to valuate, it is not surprising that a higher level of intangibles is correlated with higher audit fees. To check if this leads to problems of multicollinearity, we next calculate variance inflation factors (VIF) for the variables used in the regression model, the highest of which is 4.42. Values under five suggest moderate multicollinearity, which may not be problematic. These results serve to ease concerns over severe multicollinearity adversely impacting our inferences.

Table 4. Panel A: Correlation Variables LNAUDITFES to SEGMENTS.

	Variables	1	2	3	4	5	6	7	8	9	10	11	12	13
1	*LNAUDITFEES*	1.00												
2	*CYBER_INSURANCE*	0.08	1.00											
3	*BREACH*	0.09	0.03	1.00										
4	*INTANGIBLES*	0.74	0.08	0.09	1.00									
5	*TECHNOLOGY*	0.12	0.01	0.03	0.11	1.00								
6	*RISK*	0.14	0.04	0.04	0.15	0.04	1.00							
7	*COMPLIANCE*	0.08	0.04	0.04	0.09	0.03	0.12	1.00						
8	*LNASSETS*	0.85	0.08	0.08	0.68	0.09	0.23	0.10	1.00					
9	*DISTRESS*	-0.02	0.00	0.00	-0.02	0.00	-0.01	0.00	-0.03	1.00				
10	*INVRECV*	-0.05	-0.01	0.00	-0.03	-0.01	0.18	0.06	0.08	-0.02	1.00			
11	*LEVERAGE*	0.18	0.02	0.02	0.16	0.00	-0.03	0.01	0.13	0.07	-0.16	1.00		
12	*ROA*	0.49	0.04	0.03	0.39	0.03	0.07	0.05	0.66	-0.12	0.17	-0.01	1.00	
13	*SEGMENTS*	0.22	-0.02	0.01	0.18	0.03	-0.13	-0.05	0.08	0.00	-0.22	0.09	0.11	1.00
14	*GC*	-0.46	-0.04	-0.03	-0.32	-0.04	-0.08	-0.05	-0.57	0.08	-0.12	0.01	-0.68	-0.10
15	*LOSS*	-0.35	-0.05	-0.04	-0.36	-0.03	-0.12	-0.05	-0.48	0.10	-0.18	0.02	-0.53	-0.06
16	*FOREIGN*	0.25	-0.02	-0.01	0.21	0.03	-0.06	-0.03	0.16	0.00	-0.08	-0.03	0.11	0.10
17	*YE*	0.10	0.03	-0.01	0.04	0.00	0.06	0.04	0.14	-0.01	-0.05	0.07	0.03	-0.07
18	*CHANGE*	-0.18	-0.01	-0.02	-0.13	-0.03	-0.02	-0.01	-0.18	0.02	0.02	-0.04	-0.12	-0.03
19	*BIG4*	0.68	0.05	0.05	0.48	0.07	0.07	0.03	0.58	-0.04	-0.18	0.14	0.34	0.18
20	*IC*	0.07	0.01	-0.01	0.03	0.01	-0.01	0.01	0.03	0.00	0.00	0.02	0.02	0.02
21	*SPECIALIST*	-0.38	-0.03	-0.02	-0.23	-0.05	-0.08	-0.03	-0.36	0.02	0.02	-0.05	-0.21	-0.03
22	*CR*	-0.14	-0.05	-0.02	-0.17	0.01	-0.11	-0.04	-0.17	-0.02	-0.20	-0.18	0.00	0.05
23	*BTM*	0.11	0.01	-0.01	0.05	-0.02	0.12	0.04	0.33	-0.05	0.22	-0.21	0.33	-0.06
24	*RESTATE*	-0.01	0.01	0.00	-0.02	0.00	0.01	0.01	-0.01	0.00	0.01	0.00	0.00	0.04
25	*DELAY*	-0.44	-0.06	-0.06	-0.35	-0.09	-0.12	-0.06	-0.47	0.03	0.03	-0.09	-0.33	-0.09
26	*LAMBDA*	-0.43	-0.17	-0.06	-0.40	-0.05	-0.16	-0.12	-0.48	-0.07	-0.01	-0.09	-0.34	0.05

Table 4. Panel B: Correlation Variables GC to LAMBDA.

	Variables	14	15	16	17	18	19	20	21	22	23	24	25	26
14	*GC*	1.00												
15	*LOSS*	0.40	1.00											
16	*FOREIGN*	-0.09	-0.03	1.00										
17	*YE*	-0.06	0.00	-0.03	1.00									
18	*CHANGE*	0.13	0.09	-0.05	-0.02	1.00								
19	*BIG4*	-0.34	-0.23	0.23	0.09	-0.22	1.00							
20	*IC*	-0.01	0.03	0.04	0.00	0.03	0.02	1.00						
21	*SPECIALIST*	0.26	0.15	-0.11	-0.09	0.19	-0.46	0.00	1.00					
22	*CR*	-0.10	0.13	0.07	-0.04	0.00	-0.01	0.00	0.01	1.00				
23	*BTM*	-0.34	-0.22	-0.02	0.05	-0.01	0.02	-0.01	-0.07	-0.04	1.00			
24	*RESTATE*	-0.01	0.00	-0.03	0.01	0.02	-0.02	0.02	0.00	-0.02	0.01	1.00		
25	*DELAY*	0.35	0.29	0.00	-0.03	0.16	-0.36	0.08	0.24	0.01	-0.06	0.01	1.00	
26	*LAMBDA*	0.31	0.28	0.05	-0.18	0.07	-0.29	-0.02	0.22	0.33	-0.08	-0.05	0.34	1.00

 doi:10.20944/preprints202601.1813.v1

The choice of a firm disclosing the presence of a cyber insurance policy introduces a possible self-selection bias into our analysis. We control for potential self-selection bias by including the Heckman variable (*LAMBDA*). The results of the first stage regression are presented in Table 5. We include *LAMBDA* in our main analysis. We estimate a significant coefficient forour exclusion variable *INTANGIBLES*, thus providing support for our choice. This is consistent with the results of Smith, et al. (2019)—in their case, they were testing the probability of a breach where we are testing the probability of that a firm will disclose the acquisition of cyber insurance. The area under the ROC curve of 0.882 suggests this model explains a significant amount of the variation in the disclosure of cyber insurance.

Table 5. First Stage Determinants of Insurance Disclosure (Calculate the Inverse Mill Ratio).

$$Prob(CYBER\_INSURANCE = 1) = \gamma_0 + \gamma_1 INTANGIBLES_{it} + \gamma_2 TECHNOLOGY_{it} + \gamma_3 RISK_{it} + \gamma_4 COMPLIANCE_{it} + \gamma_5 BREACH_{it-1} + \gamma_6 LNASSETS_{it} + \gamma_7 DISTRESS_{it} + \gamma_8 INVRECV_{it} + \gamma_9 LEVERAGE + \gamma_{10} ROA_{it} + \gamma_{11} SEGMENTS_{it} + \gamma_{12} GC_{it} + \gamma_{13} LOSS_{it} + \gamma_{14} FOREIGN_{it} + \gamma_{15} YE_{it} + \gamma_{16} CHANGE_{it} + \gamma_{17} BIG4_{it} + \gamma_{18} IC_{it} + \gamma_{19} SPECIALIST_{it} + \gamma_{20} CR_{it} + \gamma_{21} BTM_{it} + \gamma_{22} RESTATE_{it} + \gamma_{23} DELAY_{it} + \varepsilon_{it}$$

	Dependent Variable: CYBER_INSURANCE		
Variable	**Coeff.**		**p-value**
INTANGIBLES	0.016	**	(0.033)
TECHNOLOGY	-0.040		(0.639)
RISK	-0.080		(0.146)
COMPLIANCE	0.234	***	(0.000)
$BREACH_{t-1}$	0.263	**	(0.036)
LNASSETS	0.034	***	(0.002)
DISTRESS	0.005		(0.350)
INVRECV	-0.345	***	(0.000)
LEVERAGE	-0.306	***	(0.000)
ROA	0.353	***	(0.001)
SEGMENTS	0.027	*	(0.057)
GC	-0.210	**	(0.037)
LOSS	0.060		(0.140)
FOREIGN	-0.123	***	(0.001)
YE	0.219	***	(0.000)
CHANGE	-0.015		(0.811)
BIG4	0.126	***	(0.008)
IC	0.038		(0.643)
SPECIALIST	-0.059		(0.513)
CR	-0.066	***	(0.000)
BTM	-0.121	***	(0.001)
RESTATE	0.199	***	(0.000)
DELAY	-2.993	***	(0.000)
Intercept			
Year Indicators	Yes		
Industry Indicators	Yes		
Area under ROC	0.882		
Pseudo R^2	0.220		
N	61,227		

* p < 0.10, ** p < 0.05, *** p < 0.01.

 doi:10.20944/preprints202601.1813.v1

Table 6 presents the result for our test of H1 that examines the association between the presence of a cyber insurance policy and audit fees on our full sample, both with and without the *LAMBDA* variable. Our variable of interest is *CYBER_INSURANCE*. The coefficient in Column (1) Table 6 is positive and significant, which suggests that firms that disclose the presence of a cyber insurance policy pay higher audit fees. Column (2) Table 6 presents the regression with *LAMBDA*. After controlling for selection-bias, we find, consistent with the results presented in Column (1), a positive and significant coefficient on *CYBER_INSURANCE*. We also estimate a significant coefficient designed to capture the likelihood of a firm reporting cyber insurance (negative), providing additional support for the use of *LAMBDA*. These results reveal that the disclosure of a cyber insurance policy is associated with a 3.9% increase in audit fees.

Table 6. The Association Between Cyber Insurance and Audit Fees.

$$\begin{aligned} LNAUDITFEES = {} & \beta_0 + \beta_1 CYBER\_INSURANCE_{it} + \beta_2 TECHNOLOGY_{it} + \beta_3 RISK_{it} \\ & + \beta_4 COMPLIANCE_{it} + \beta_5 BREACH_{it-1} + \beta_6 LNASSETS_{it} + \beta_7 DISTRESS_{it} \\ & + \beta_8 INVRECV_{it} + \beta_9 LEVERAGE + \beta_{10} ROA_{it} + \beta_{11} SEGMENTS_{it} + \beta_{13} GC_{it} \\ & + \beta_{13} LOSS_{it} + \beta_{14} FOREIGN_{it} + \beta_{15} YE_{it} + \beta_{16} CHANGE_{it} + \beta_{17} BIG4_{it} + \beta_{18} IC_{it} \\ & + \beta_{19} SPECIALIST_{it} + \beta_{20} CR_{it} + \beta_{21} BTM_{it} + \beta_{22} RESTATE_{it} + \beta_{23} DELAY_{it} + \varepsilon_{it} \end{aligned}$$

	Dependent Variable: LNAUDITFEES					
	(1) OLS			(2) Heckman		
Variable	Coeff.		p-value	Coeff.		p-value
CYBER_INSURANCE	0.032	*	(0.082)	0.039	**	(0.034)
TECHNOLOGY	0.145	***	(0.000)	0.155	***	(0.000)
RISK	0.090	***	(0.000)	0.115	***	(0.000)
COMPLIANCE	0.081	***	(0.000)	-0.001		(0.967)
$BREACH_{t-1}$	0.206	***	(0.000)	0.112	***	(0.007)
LNASSETS	0.494	***	(0.000)	0.480	***	(0.000)
DISTRESS	-0.002	***	(0.000)	-0.004	***	(0.000)
INVRECV	0.248	***	(0.000)	0.380	***	(0.000)
LEVERAGE	0.001	*	(0.084)	0.001	*	(0.087)
ROA	-0.441	***	(0.000)	-0.576	***	(0.000)
SEGMENTS	0.022	***	(0.000)	0.012	***	(0.000)
GC	-0.038	***	(0.003)	0.034	**	(0.018)
LOSS	0.084	***	(0.000)	0.067	***	(0.000)
FOREIGN	0.094	***	(0.000)	0.134	***	(0.000)
YE	0.012	*	(0.063)	-0.067	***	(0.000)
CHANGE	-0.006		(0.583)	-0.001		(0.931)
BIG4	0.418	***	(0.000)	0.369	***	(0.000)
IC	0.342	***	(0.000)	0.329	***	(0.000)
SPECIALIST	-0.245	***	(0.000)	-0.226	***	(0.000)
CR	-0.022	***	(0.000)	0.002		(0.486)
BTM	-0.195	***	(0.000)	-0.164	***	(0.000)
RESTATE	0.045	***	(0.000)	-0.027	**	(0.017)
DELAY	-0.029	***	(0.009)	0.068	***	(0.000)
LAMBDA				-0.398	***	(0.000)
Intercept	10.439	***	(0.000)	11.765	***	(0.000)
Year Indicators	Yes			Yes		
Industry Indicators	Yes			Yes		
Adjusted R^2	0.868			0.868		
N	61,227			61,227		

 doi:10.20944/preprints202601.1813.v1

* p < 0.10, ** p < 0.05, *** p < 0.01.

We also control for self-selection bias by creating a matched sample based on the predicted probabilities from the first-stage regression (Table 5), also known as a propensity score matching, to control for differences between firms with and without the cyber insurance disclosure. The propensity score matching controls for factors related with firms choosing to disclose a cyber insurance policy and for firm performance. Table 7 presents the difference in means between the treatment and control group. There are no significant differences between the two groups, consistent with an effective matching procedure. Our PSM results, presented in Table 8, are similar to those presented in Table 6. These results again indicate that companies with *CYBER_INSURANCE* pay higher audit fees (an approximately 9% premium).

Table 7. Comparison of Cyber Insurance and Propensity Scored Matched Non-Cyber Insurance Observations.

Variable	Treated (n=1,043)	Control (n=1,043)	Difference	p-value
LNAUDITFEES	14.384	14.420	-0.036	0.832
TECHNOLOGY	0.033	0.033	-0.001	0.975
RISK	0.112	0.100	0.012	0.771
COMPLIANCE	0.078	0.100	-0.022	0.533
$BREACH_{t-1}$	0.019	0.033	-0.014	0.446
LNASSETS	7.845	8.039	-0.194	0.492
DISTRESS	-2.974	-2.976	0.001	0.996
INVRECV	0.232	0.220	0.012	0.681
LEVERAGE	0.232	0.229	0.003	0.935
ROA	0.039	0.062	-0.023	0.261
SEGMENTS	1.614	1.582	0.032	0.842
GC	0.019	0.017	0.003	0.890
LOSS	0.236	0.167	0.069	0.217
FOREIGN	0.256	0.267	-0.011	0.854
YE	0.867	0.900	-0.033	0.459
CHANGE	0.052	0.083	-0.032	0.291
BIG4	0.803	0.850	-0.047	0.376
IC	0.034	0.067	-0.033	0.177
SPECIALIST	0.066	0.058	0.008	0.732
CR	1.135	0.949	0.186	0.343
BTM	0.431	0.389	0.041	0.415
RESTATE	0.099	0.067	0.032	0.415
DELAY	4.085	4.094	-0.009	0.781

Table 8. The Association of Cyber Insurance and Audit Fees (PSM).

$$LNAUDITFEES = \beta_0 + \beta_1 CYBER\_INSURANCE_{it} + \beta_2 TECHNOLOGY_{it} + \beta_3 RISK_{it} + \beta_4 COMPLIANCE_{it} + \beta_5 BREACH_{it-1} + \beta_6 LNASSETS_{it} + \beta_7 DISTRESS_{it} + \beta_8 INVRECV_{it} + \beta_9 LEVERAGE + \beta_{10} ROA_{it} + \beta_{11} SEGMENTS_{it} + \beta_{13} GC_{it} + \beta_{13} LOSS_{it} + \beta_{14} FOREIGN_{it} + \beta_{15} YE_{it} + \beta_{16} CHANGE_{it} + \beta_{17} BIG4_{it} + \beta_{18} IC_{it} + \beta_{19} SPECIALIST_{it} + \beta_{20} CR_{it} + \beta_{21} BTM_{it} + \beta_{23} RESTATE_{it} + \beta_{23} DELAY_{it} + \varepsilon_{it}$$

	Dependent Variable: LNAUDITFEES		
Variable	**Coeff.**		**p-value**
CYBER_INSURANCE	0.091	***	(0.000)
TECHNOLOGY	0.182	**	(0.016)
RISK	0.012		(0.786)

 doi:10.20944/preprints202601.1813.v1

COMPLIANCE	0.004		(0.934)
$BREACH_{t-1}$	0.182	*	(0.053)
LNASSETS	0.476	***	(0.000)
DISTRESS	-0.003		(0.850)
INVRECV	-0.225	***	(0.002)
LEVERAGE	0.030		(0.762)
ROA	0.087		(0.524)
SEGMENTS	0.115	***	(0.000)
GC	0.143		(0.358)
LOSS	0.239	***	(0.000)
FOREIGN	0.268	***	(0.000)
YE	0.002		(0.951)
CHANGE	-0.063		(0.337)
BIG4	0.577	***	(0.000)
IC	0.498	***	(0.000)
SPECIALIST	0.137		(0.163)
CR	0.035	***	(0.006)
BTM	-0.350	***	(0.000)
RESTATE	-0.028		(0.560)
DELAY	0.068		(0.430)
Intercept	8.809	***	(0.000)
Year Indicators	Yes		
Industry Indicators	Yes		
Adjusted R^2	0.793		
N	2,086		

* p < 0.10, ** p < 0.05, *** p < 0.01.

To test H2 whether the disclosure of an existing cyber insurance policy after a reported cybersecurity incident is associated with audit fees, we add an indicator variable *POST_BREACH. POST_BREACH* set equal to one if the observation falls in a period subsequent to the data breach, otherwise it is set equal to zero. We also include the interaction of *POST_BREACH* and *CYBER_INSURANCE.*

Our regression results for these tests are presented in Table 9. Here, the *CYBER_INSURANCE* and *POST_BREACH* variables are positively and significantly associated with audit fees. The coefficient for the main effect of *CYBER_INSURANCE* and *POST_BREACH* is, however, negative and significantly associated with lower audit fees. To determine how the disclosure of a cyber insurance policy affects audit fees in the post breach period, we conduct a joint test of the coefficients for *CYBER_INSURANCE* and *CYBER_INSURANCE * POST_BREACH*. The joint test is negative and significant ($\delta_1 + \delta_3 = -0.156$, p-value = 0.071). This result indicates that firms disclosing a cyber insurance policy after experiencing a data breach pay lower audit fees (i.e., the auditor has a lower risk assessment relative to firms without cyber insurance). As an additional robustness check on H2, we use our matched sample firms to control for observable differences between firms with a cyber insurance policy and those without so that our conclusions are not biased. The results of these tests are presented in Table 10. Consistent with our initial results, the coefficient of the interaction of *CYBER_INSURANCE* and *POST_BREACH* is negative, with the magnitude being nearly twice as large, and significantly associated with lower audit fees. The findings reported in Table 9 and 10 provide robust proof for H2.

 doi:10.20944/preprints202601.1813.v1

Table 9. Post Data Breach Difference-in-Difference Regression of Cyber Insurance on Audit Fees.

$$LNAUDITFEES = \delta_0 + \delta_1 CYBER\_INSURANCE_{it} + \delta_2 POST\_BREACH_{it} + \delta_3 CYBER\_INSURANCE * POST\_BREACH_{it} + \delta_4 TECHNOLOGY_{it} + \delta_5 RISK_{it} + \delta_6 COMPLIANCE_{it} + \delta_7 BREACH_{it-1} + \delta_8 LNASSETS_{it} + \delta_9 DISTRESS_{it} + \delta_{10} INVRECV_{it} + \delta_{11} LEVERAGE + \delta_{12} ROA_{it} + \delta_{13} SEGMENTS_{it} + \delta_{14} GC_{it} + \delta_{15} LOSS_{it} + \delta_{16} FOREIGN_{it} + \delta_{17} YE_{it} + \delta_{18} CHANGE_{it} + \delta_{19} BIG4_{it} + \delta_{20} IC_{it} + \delta_{21} SPECIALIST_{it} + \delta_{22} CR_{it} + \delta_{23} BTM_{it} + \delta_{24} RESTATE_{it} + \delta_{25} DELAY_{it} + \delta_{25} LAMBDA_{it} + \varepsilon_{it}$$

	Dependent Variable: LNAUDITFEES		
Variable	**Coeff.**		**p-value**
CYBER_INSURANCE	0.042	**	(0.032)
POST_BREACH	0.192	***	(0.000)
*CYBER_INSURANCE * POST_BREACH*	-0.107	*	(0.069)
TECHNOLOGY	0.150	***	(0.000)
RISK	0.108	***	(0.000)
COMPLIANCE	-0.005		(0.778)
$BREACH_{t-1}$	-0.053		(0.239)
LNASSETS	0.479	***	(0.000)
DISTRESS	-0.004	***	(0.000)
INVRECV	0.382	***	(0.000)
LEVERAGE	0.001	*	(0.088)
ROA	-0.574	***	(0.000)
SEGMENTS	0.012	***	(0.000)
GC	0.033	**	(0.024)
LOSS	0.068	***	(0.000)
FOREIGN	0.136	***	(0.000)
YE	-0.066	***	(0.000)
CHANGE	-0.001		(0.957)
BIG4	0.370	***	(0.000)
IC	0.330	***	(0.000)
SPECIALIST	-0.228	***	(0.000)
CR	0.002		(0.453)
BTM	-0.161	***	(0.000)
RESTATE	-0.027	**	(0.019)
DELAY	0.070	***	(0.000)
LAMBDA	-0.400	***	(0.000)
Intercept	11.775	***	(0.000)
Year Indicators	Yes		
Industry Indicators	Yes		
Adjusted R^2	0.869		
N	61,227		

* p < 0.10, ** p < 0.05, *** p < 0.01.

Table 10. Post Data Breach Difference-in-Difference Regression of Cyber Insurance on Audit Fees (PSM).

	Dependent Variable: LNAUDITFEES		
Variable	**Coeff.**		**p-value**
CYBER_INSURANCE	0.051	*	(0.085)
POST_BREACH	0.182	**	(0.012)
*CYBER_INSURANCE * POST_BREACH*	-0.207	**	(0.026)
TECHNOLOGY	0.338	***	(0.000)

 doi:10.20944/preprints202601.1813.v1

RISK	0.201	***	(0.003)
COMPLIANCE	-0.637	***	(0.000)
$BREACH_{t-1}$	-0.482	***	(0.006)
LNASSETS	0.396	***	(0.000)
DISTRESS	-0.022		(0.342)
INVRECV	0.923	***	(0.000)
LEVERAGE	0.787	***	(0.001)
ROA	-1.202	***	(0.000)
SEGMENTS	-0.097	***	(0.000)
GC	0.592	***	(0.004)
LOSS	0.018		(0.724)
FOREIGN	0.413	***	(0.000)
YE	-0.615	***	(0.000)
CHANGE	0.055		(0.431)
BIG4	0.116		(0.160)
IC	0.317	***	(0.000)
SPECIALIST	0.144		(0.166)
CR	0.198	***	(0.000)
BTM	0.176	**	(0.046)
RESTATE	-0.553	***	(0.000)
DELAY	0.787	***	(0.000)
Intercept	18.565	***	(0.000)
Year Indicators	Yes		
Industry Indicators	Yes		
Adjusted R^2	0.833		
N	2,086		

* p < 0.10, ** p < 0.05, *** p < 0.01.

Next, we examine the association between cyber security and future breaches. Even when businesses invest in cybersecurity measures and systems and hire teams of security professionals to operate these systems, some risk remains, residual risks. Many firms choose a pragmatic approach to residual risks and transfer the risk of a cyber breach to an insurance company for a fee. There is also the concern that risk disclosures may provide information to hackers. We test whether cyber insurance disclosure is associated with future breaches (H3). This test is of concern because the disclosure of a cyber insurance policy should lower residual risks and risks that might contain information for hackers seeking high risk targets. The results of these tests are presented in Table 11. *CYBER_INSURANCE* is not significantly associated, either positively or negatively, with future data breaches.

Table 11. Cybersecurity Insurance and Future Cyber Security Breaches (PSM).

$$BREACH_{t+1} = \alpha_0 + \alpha_1 CYBER\_INSURANCE_{it} + \alpha_2 TECHNOLOGY_{it} + \alpha_3 RISK_{it} + \alpha_4 COMPLIANCE_{it} + \alpha_5 BREACH_{it-1} + \alpha_6 LNASSETS_{it} + \alpha_7 LOSS_{it} + \alpha_8 LEVERAGE + \alpha_9 INTANGIBLES_{it} + \alpha_{10} SEGMENTS_{it} + \varepsilon_{it}$$

	Dependent Variable: $BREACH_{t+1}$		
Variable	**Coeff.**		**p-value**
CYBER_INSURANCE	-0.141		(0.496)
TECHNOLOGY	1.103	***	(0.002)
RISK	-0.200		(0.432)
COMPLIANCE	0.395		(0.333)
$BREACH_{t-1}$	0.809	***	(0.002)
LNASSETS	0.129	**	(0.031)

 doi:10.20944/preprints202601.1813.v1

LOSS	-0.885	***	(0.009)
LEVERAGE	-0.009		(0.982)
INTANGIBLES	-0.003		(0.956)
SEGMENTS	0.060		(0.442)
Intercept	-3.567	***	(0.000)
Year Indicators	Yes		
Industry Indicators	Yes		
Pseudo R^2	0.833		
N	2,086		

* p < 0.10, ** p < 0.05, *** p < 0.01.

But what if the firm has a diligent internal audit committees, one with cyber security oversight? Does this change the effect of cyber insurance on future breaches? The answer appears to be yes. Table 12 presents the results for H4, that tests the association of cyber insurance and the audit committee cybersecurity oversight responsibilities with audit fees. Smith, et al. (2019) finds that firms with more active audit committees experience lower audit fee premiums. Outside auditors being less inclined to price breach risk when firms have diligent internal governance mechanisms in place. Our variable of interest is *AUDITCOMMITTEECYBEROVER* which is 1 if a company's audit committee charter provides a provision regarding cybersecurity oversight. We find that firms that disclose having cyber insurance in the post breach period lower their audit premiums by 8.7%. This is a statistically and economically significant result. This result suggests that firms where the audit committee has cyber security oversight duties are charged lower audit fees by their auditor. This supports the notion that stronger governance is associated with lower fees.

Table 12. Post Data Breach Difference-in-Difference Regression of Cyber Insurance and Audit Committee Cybersecurity Oversight Duties on Audit Fees.

$$\begin{aligned} LNAUDITFEES = {} & \delta_0 + \delta_1 CYBER\_INSURANCE_{it} + \delta_2 POST\_BREACH_{it} \\ & + \delta_3 CYBER\_INSURANCE * POST\_BREACH_{it} \\ & + \delta_4 AUDITCOMMITTEECYBEROVER + \delta_5 TECHNOLOGY_{it} + \delta_6 RISK_{it} \\ & + \delta_7 COMPLIANCE_{it} + \delta_8 BREACH_{it-1} + \delta_9 LNASSETS_{it} + \delta_{10} DISTRESS_{it} \\ & + \delta_{11} INVRECV_{it} + \delta_{12} LEVERAGE + \delta_{13} ROA_{it} + \delta_{14} SEGMENTS_{it} + \delta_{15} GC_{it} \\ & + \delta_{16} LOSS_{it} + \delta_{17} FOREIGN_{it} + \delta_{18} YE_{it} + \delta_{19} CHANGE_{it} + \delta_{20} BIG4_{it} + \delta_{21} IC_{it} \\ & + \delta_{22} SPECIALIST_{it} + \delta_{23} CR_{it} + \delta_{24} BTM_{it} + \delta_{25} RESTATE_{it} + \delta_{26} DELAY_{it} + \varepsilon_{it} \end{aligned}$$

	Dependent Variable: LNAUDITFEES		
Variable	**Coeff.**		**p-value**
CYBER_INSURANCE	0.054	*	(0.071)
POST_BREACH	0.245	***	(0.000)
*CYBER_INSURANCE * POST_BREACH*	-0.230	**	(0.012)
AUDITCOMMITTEECYBEROVER	-0.087	***	(0.004)
TECHNOLOGY	0.346	***	(0.000)
RISK	0.201	***	(0.002)
COMPLIANCE	-0.657	***	(0.000)
BREACHt-1	-0.519	***	(0.003)
LNASSETS	0.393	***	(0.000)
DISTRESS	-0.023		(0.313)
INVRECV	0.949	***	(0.000)
LEVERAGE	0.797	***	(0.001)
ROA	-1.220	***	(0.000)
SEGMENTS	-0.099	***	(0.000)
GC	0.592	***	(0.003)

 doi:10.20944/preprints202601.1813.v1

LOSS	0.014		(0.775)
FOREIGN	0.414	***	(0.000)
YE	-0.627	***	(0.000)
CHANGE	0.051		(0.466)
BIG4	0.115		(0.162)
IC	0.316	***	(0.000)
SPECIALIST	0.144		(0.168)
CR	0.201	***	(0.000)
BTM	0.180	**	(0.039)
RESTATE	-0.554	***	(0.000)
DELAY	0.796	***	(0.000)
Intercept	18.801	***	(0.000)
Year Indicators	Yes		
Industry Indicators	Yes		
Adjusted R2	0.834		
N	2,086		

* p < 0.10, ** p < 0.05, *** p < 0.01.

5. Conclusions

We investigate whether auditors adjust their business risk assessments when client firms purchase cyber insurance products, specifically the association between the purchase of cyber insurance and audit fees. We find that overall, while firms that purchase cyber insurance experience higher audit fees. This is likely the result of an overall greater risk profile for those firms that deem it prudent to purchase this product. We control for endogeneity via both an instrumental variable approach and via propensity score matching. Neither method produces results that differ from those reported above.

We also find that after a breach, the disclosure of an existing cyber insurance policy is associated with lower audit fees. This is no doubt because the auditor was aware of the policy and thus reduced the company's risk assessment relative to other high-risk firms without such policies. Finally, we find that firms where the audit committee has cyber security oversight duties are charged lower audit fees by their auditor. We conclude that the purchase of cyber insurance is indicative of an overall higher risk profile, but that having that insurance after experiencing a breach reduces perceived risk. Similarly, assignment of risk oversight to the audit committee reduces perceived risk. Together these results should provide guidance to firms and regulators as they seek to address and mitigate the business risks associated with information technology.

References

Aon Empower Results. (2019). US Cyber Market Update: 2018 US Cyber Insurance Profit and Performance. Available at http://thoughtleadership.aon.com/Documents/201906-us-cyber-market-update.pdf

Allianz. (2015). A guide to cyber risk. Managing the impact of increasing interconnectivity. Available at https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-guide.html

Amir, E., Levi, S., and Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177-1206. https://doi.org/10.1007/s11142-018-9452-4

Bell, T. B., W. R. Landsman, and D. A. Shackelford. (2001). Auditors' perceived business risk and audit fees: Analysis and evidence. *Journal of Accounting Research* 39: 35–43. http://www.jstor.org/stable/2672944

Biener, C., Eling, M., and J. Hendrick Wirfs (2015) Insurability of cyber risk: An empirical analysis. *The Geneva Papers n Risk and Insurance – Issues and Practice* 40:131-158/ http://www.jstor.org/stable/24736570

Böhme, R.(2005). Cyber-insurance Revisited. in *Proceedings of Workshop on the Economics of Information Security (WEIS)*, 2005.

Brumfield. C. A., R. K. Elliott, and P. D. Jacobson. (1983). Business risk and the audit process. *Journal of Accountancy* 155: 60–68. https://api.semanticscholar.org/CorpusID:15524306

 doi:10.20944/preprints202601.1813.v1

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53-63. https://doi.org/10.1080/23738871.2017.1296878

Campbell, J. L., Chen, H., Dhaliwal, D. S., Lu, H. M., and Steele, L. B. (2014). The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies*, 19(1), 396-455. https://doi.org/10.1007/s11142-013-9258-3

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70-104. http://www.jstor.org/stable/27751132

Chang, H., Ho, L.C., Liu, Z, and Ouyang, B. (2021). Income smoothing and audit fees. *Advances in Accounting, 54*, 100547. https://doi.org/10.1016/j.adiac.2021.100547

Du, S., Xu, X., and Yu, K. (2020). Does corporate social responsibility affect auditor-client contracting? Evidence from auditor selection and audit fees. *Advances in Accounting, 51*, 100499. https://doi.org/10.1016/j.adiac.2020.100499

Ettredge, M. L., and Richardson, V. J. (2003). Information transfer among internet firms: the case of hacker attacks. *Journal of Information Systems*, *17*(2), 71-82. https://www.proquest.com/scholarly-journals/information-transfer-among-internet-firms-case/docview/235947408/se-2

Gatzert, N., and Schubert, M. (2022) Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. *The Journal of Risk and Insurance, 89*: 725-763. https://doi.org/10.1111/jori.12381

Gazert, N., Schmit, J., and Kolb, A., (2016) Assessing the risks of insuring reputation risk. *The Journal of Risk and Insurance* 83(3): 641-679. https://doi.org/10.1111/jori.12065

Gordon, L. A., Loeb, M. P., and Sohail, T. 2003. A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81-85. DOI: 10.1145/636772.636774

Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, 25(5), 503-530. https://doi.org/10.1016/j.jaccpubpol.2006.07.005

Guttman, B., and Roback, E. A. (1995). *An introduction to computer security: the NIST handbook*. DIANE Publishing. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Heckman, J. J. 1979. Sample selection bias as a specification error. *Econometrica* 47 (February): 153–162. https://doi.org/10.2307/1912352

Higgs, J. L., Robert E. P., Thomas J. S., and George R. Y. 2016. The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems* 30, (3): 79-98. https://doi.org/10.2308/isys-51402

Hoo, K. J. S. (2000). *How much is enough? A risk management approach to computer security*. Stanford: Stanford University. https://cisac.fsi.stanford.edu/publications/how_much_is_enough__a_riskmanagement_approach_to_computer_security

Kannan, K., Rees, J., and Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, *12*(1), 69-91. https://doi.org/10.2753/JEC1086-4415120103

Kesan, J., Majuca, R., and Yurcik, W. (2005, June). Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study. *Workshop on the Economics of Information Security* (pp. 1-46). *https://api.semanticscholar.org/CorpusID:212684768*

Koh, K., and Tong, Y. H. (2012). The effects of clients' controversial activities on audit pricing. *Auditing: A Journal of Practice & Theory*, *32*(2), 67-96. https://doi.org/10.2308/ajpt-50348

Li, He, No, Won Gyun and J. Efrim Boritz (2020) Are external auditors concerned about cyber incidents? Evidence from audit fees. *AUDITING: A Journal of Practice & Theory* 39 (1): 151–171. https://doi.org/10.2308/ajpt-52593

Li, H., No, W. G., and Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30, 40-55. https://doi.org/10.1016/j.accinf.2018.06.003

 doi:10.20944/preprints202601.1813.v1

Lyon, J. D., and Maher, M. W. (2005). The importance of business risk in setting audit fees: Evidence from cases of client misconduct. *Journal of Accounting Research*, 43(1), 133-151. https://doi.org/10.1111/j.1475-679x.2005.00165.x

Majuca, R. P., Yurcik, W., and Kesan, J. P. (2006). The evolution of cyberinsurance. *https://arxiv.org/abs/cs/0601020*

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11-26. https://doi.org/10.1016/j.dss.2013.04.004

Ponemon Institute and IBM Security. (2019). Cost of a data breach report 2019. Available at https://www.ibm.com/security/data-breach

Richardson, V., Watson, M. W., and Smith, R. E. (2019). Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems* 33 (3): 227–265. https://doi.org/10.2308/isys-52379

Risk Based Security. (2019). Data breach quick view report 2018. Available at https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report

Securities and Exchange Commission (2005) Securities Act Rel. No. 33-8591, *Securities Offering Reform*. https://www.sec.gov/files/rules/final/33-8591.pdf

Securities and Exchange Commission. (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. February 26, 2018. https://www.govinfo.gov/app/details/FR-2018-02-26/2018-03858/summary

Sellers, R.D., Fogarty,J., and Jadallah, J. 2020. Has the new world order taught the big four to manage client portfolio risk? Examining extreme loss occurrences before and after Sarbanes Oxley. *Advances in Accounting*, Volume 51. https://doi.org/10.1016/j.adiac.2020.100498

Schrader, C. and Sun, H. (2019). How does the type of equity compensation of audit committee affect audit fees? *Advances in Accounting 45,* 100411. https://doi.org/10.1016/j.adiac.2019.02.001

Shackelford, S. (2012). Should your firm invest in cyber insurance? *Business Horizons* 55: 349-356. https://doi.org/10.1016/j.bushor.2012.02.004

Smith, T., Higgs, J. L., and Pinsker, R. (2019). Do Auditors Price Breach Risk in Their Audit Fees? *Journal of Information Systems,* 33(2), 177-204. https://doi.org/10.2308/isys-52241

Swiss Re. (2017). Cyber: getting to grips with a complex risk. Sigma 1/2017. https://www.swissre.com/dam/jcr:995517ee-27cd-4aae-b4b1-44fb862af25e/sigma1_2017_en.pdf

Vacca, J. R. (2012). *Computer and information security handbook*. Newnes. https://www.sciencedirect.com/book/edited-volume/9780123943972/computer-and-information-security-handbook

Wang, T., Kannan, K. N., and Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, 24(2), 201-218. http://www.jstor.org/stable/42004301

Xie, X., Lee, C., and Eling M. (2019). Cyber insurance supply and performance: an analysis of the U.S. cyber insurance market. *Geneva Pap Risk Insur Issues Pract* **45**, 690–736 (2020). https://doi.org/10.1057/s41288-020-00176-5

Yen, J. C., Lim, J. H., Wang, T., and Hsu, C. (2018). The impact of audit firms' characteristics on audit fees following information security breaches. *Journal of Accounting and Public Policy*, *37*(6), 489-507. https://doi.org/10.1016/j.jaccpubpol.2018.10.002.