Ahead of the Breach: Anticipatory Approaches to Mitigating Ex-post Costs of Cyber Breaches*

Ndackyssa Oyima-Antseleve

December 20, 2023

Abstract

This study critically evaluates the proactive cybersecurity strategies of managers in publicly traded companies, leveraging a unique dataset of actual cybersecurity risk measures from a leading cybersecurity scores company. I find that managers exhibit an awareness of their cybersecurity risks and engage in preemptive actions to either enhance their cyber defenses, acquire cyber insurance, or increase cash reserves before a breach or some combination of these actions. This investigation reveals that while some firms bolster their cyber defenses, others opt for cyber insurance and increased cash reserves as precautionary measures. The findings indicate that cyber insurance is not complementing but rather substituting for investment in cyber defense mechanisms. This substitution raises concerns about the cyber insurance market's adverse selection and moral hazard problems.

Keywords: Cybersecurity Risk, Cyber-attacks, Cyber Insurance, Risk Management, Moral Hazard , Adverse Selection, Reputation
JEL codes: G14, G22, G32

1 Introduction

In the current business environment, the risk associated with cybersecurity has emerged as a dominant issue, overshadowing other serious concerns such as political instability and climate change-related risks. This heightened awareness is reflected in the findings of the 2021 Fortune 500 CEO Survey, where a substantial number of CEOs recognize cybersecurity threats as a top challenge to their business continuity (Jamilov, Rey, and Tahoun 2021). High-profile cyber incidents, including the 2013 Target breach that compromised the data of 40 million customers and the 2017 Equifax breach that affected 145.5 million individuals, have significantly contributed to this sense of urgency (Florackis et al. 2022). Moreover, attacks on critical infrastructure, such as the Colonial Pipeline, have amplified the gravity of cybersecurity concerns (Crosignani, Macchiavelli, and Silva 2021).

*I would like to thank Dr. Kieschnick and Dr. Zhong for their insightful comments on earlier drafts of this paper.

The scholarly response to these developments has been robust, with researchers meticulously examining the aftermath of cyber breaches, particularly those originating from external threats. Studies have analyzed various consequences, such as the impact on shareholder wealth (Gatzlaff and McCullough 2010; Kamiya et al. 2021), corporate governance (Lending, Minnick, and Schorno 2018), brand reputation (Makridis 2021), and even the cost of capital (Jiang, Yu, and Zhang 2022; Florackis et al. 2022; Jamilov, Rey, and Tahoun 2021). Further investigations have covered the influence on corporate investments and innovation (Lattanzio and Ma 2023), operations, and mergers and acquisitions activities.

On the regulatory front, agencies have increased their vigilance, proposing new standards to protect investors from cyber threats, with several measures slated for implementation by 2023 (SEC 2023, 2022, 2018, 2011). Complementarily, the Biden Administration has enacted legislation aimed at reinforcing the nation's cybersecurity framework. As a result of this heightened regulatory scrutiny and pressure from consumers and stakeholders alike, businesses have been exploring methods to mitigate such risks. The insurance industry has responded by offering cyber-risk insurance policies designed to cover a spectrum of liabilities, ranging from compliance with data breach notifications to compensations for consumer lawsuits, infrastructure repairs, and credit monitoring for those impacted.

Given the well-acknowledged importance of cyber risk in modern boardrooms and among business leaders (Bob Zukis 2021), it is expected that managers would proactively mitigate the costs associated with potential cyber attacks. They can do this in three ways.

First, they can implement internal procedures to reduce the risk of such breaches. However, the issue here is that the myriad of costs underpinning data protection serve as significant deterrents to establishing comprehensive cybersecurity infrastructures within corporations. These include the continuous expenses of administering and updating security measures, the financial burden of deciphering and advocating for industry best practices, and the ongoing oversight expenditures required once security mechanisms are operational. These substantial investments necessary for a robust cybersecurity setup often seem unjustified, especially when the financial repercussions of data breaches appear relatively minor in the grand scheme of corporate revenues.

Second, they can change their operations in a way that might mitigate some of the costs associated with a breach. For example, they might increase their cash holdings before an attack to mitigate the ex-post cash shock from a data breach.

Third, they can purchase cyber insurance to mitigate the ex-post costs associated with a data breach. For example, the notorious data breaches at Home Depot, Sony, and Target in 2014 inflicted financial damages on each company that amounted to less than one percent of their annual revenues (Michael Kassner 2015). Taking Target as a case study, the initial losses totaled $252 million due to the cyberattack. However, the financial impact was substantially mitigated by a $90 million payout from cyber insurance and an additional $57 million in tax deductions, ultimately reducing the net loss to $105 million, which is nearly 0.1% of Target's 2014 sales (Michael Kassner 2015).

Because of their exposure, one might expect insurance companies offering cyber insurance to promote firm practices to reduce the odds of a successful cyber attack. Hence, the question of whether cyber insurance promotes better cybersecurity practices among corporations remains open, given some stakeholders' doubts and concerns (Miller 2019; Bailey 2014). Especially when some stakeholders suggest it does not (Bob Zukis 2021 ; Coble 2021). However, with the increasing number of data breaches and the associated social pressures and intangible impacts such as reputational consequences also on the rise, simply cutting corners on cybersecurity hygiene is no longer a viable cost-saving strategy. This raises crucial considerations about how companies manage such risks before they materialize and cyber insurance's role in this context. Does it enhance corporate cybersecurity, or could it undermine it by providing a false sense of security?

While a rich body of literature analyzes the financial market's and management's responses to cyber incidents and the adequacy of risk pricing, the emphasis has been predominantly on post-breach reactions. Studies (Florackis et al. 2022; Lattanzio and Ma 2023; Francis, Hu, and Shohfi 2021) have touched on the ways firms adjust their investment and innovation strategies in the face of heightened pre-breach cyber risks, yet most research focuses solely on the aftermath, leaving pre-breach preparations and anticipations largely unexplored. This study builds upon and extends the inquiries of these researchers by examining the implications for cash and risk management policies conditioning on cyber insurance. It differentiates itself from prior works by leveraging actual cyber risk data from a major cybersecurity firm and adopting a comprehensive data collection methodology similar to Abbiati et al. (2021) , ensuring a representative sampling of data breaches.

The principal objective of this research is to examine the cash and risk management strategies companies employ in anticipation of data breaches or escalating cyber threats. The investigation reveals that while some firms enhance their cybersecurity measures, others increasingly rely on cyber insurance and augmented cash reserves as a buffer. Surprisingly, it emerges that firms with cyber insurance often display heightened risk profiles and are more prone to cyber-attacks. This finding suggests a dependency on insurance policies at the expense of strengthening cybersecurity defenses. Such a discovery signals a counterproductive dynamic where cyber insurance may be supplanting, rather than supporting, robust cyber defense strategies. This phenomenon raises pivotal concerns regarding moral hazard and adverse selection within the cyber insurance market, challenging the notion that insurance necessarily spurs firms to bolster their cybersecurity frameworks.

The paper is structured in the following manner. First, a comprehensive review of the existing literature is presented to contextualize the study within the broader academic discussion. Next, the research hypotheses are delineated, setting a clear trajectory for the investigation. The subsequent sections detail the data collection and research methodology to ensure a robust and replicable research design. Then, the research findings are presented and discussed. Finally, the last sections discuss the implications of the research findings, offering a reflective evaluation of their significance and contributions to the existing body of knowledge.

2 Literature Review

2.1 Cyber Breaches, Expectations and Precautionary Measures

As the fusion of technology with business operations deepens, the looming presence of cyber threats grows increasingly significant. Companies must incessantly refine their cyber risk management strategies, taking into account both the likelihood and potential impact of data breaches (Florackis et al. 2022). This entails not only assessing their current vulnerability but also forecasting future risks and preparing accordingly (Kamiya et al. 2021).

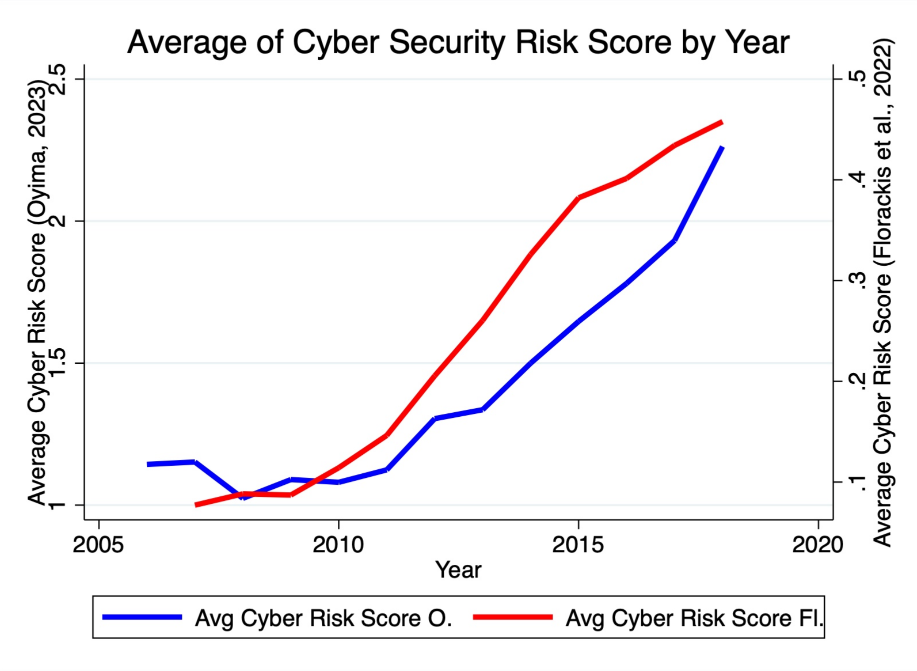


Figure 1: This graph displays the annual averages of several metrics: the cybersecurity measure I constructed and the cybersecurity measure by Florackis. It illustrates the evolution of cybersecurity risk, which appears to have increased over the years. Cyber Score Oyima is a weighted word count constructed where weights were calculated using the methodology of Loughran and McDonald (2011), following Lattanzio et al. (2023) to develop a 10-K disclosures-based measure with a comprehensive dictionary. Cyber Score Floracкis et al. (2022) is based on the 10-K cybersecurity risk measure provided by Florackis et al. (2022)

Firms with high ex-ante cyber risks are identified as being more exposed to future breaches, indicating that they are acutely aware of their cyber risk profile as discussed in their 10-K disclosures (Florackis et al. 2022). This awareness is expected to translate into comprehensive preventative measures, although the specific financial strategies firms use in anticipation of such risks have not been fully explored in the literature.

Preemptive actions are unanimously endorsed by leading scholars and regulatory bodies as critical to cybersecurity risk management (Jamilov, Rey, and Tahoun 2021). The existing body of research corroborates the need for such strategies by highlighting the severe financial consequences of cyber incidents (Janakiraman, Lim, and Rishika 2018).

Recent studies have examined the impact of cyber breaches on corporate reputation and customer trust, indicating that these incidents have tangible effects on brand value and sales (Hsu, Kao, and Wang 2021; Akey, Lewellen, and Liskovich 2018). Furthermore, large firms are shown to experience substantial financial repercussions in the wake of cyber attacks, marked by a pronounced decline in sales growth and other key financial metrics (Kamiya et al. 2021). The findings of this research align with these studies, revealing that market expectations of cyber incidents, as reflected in stock price movements, can predict subsequent sales declines (Oyima-Antseleve 2023) . This suggests that investors, and by extension, management teams, are sensitive to the severity of breaches.

Therefore, the literature suggests preventive financial management as a potential response to the threat of cyber risks. This encompasses a range of actions, from bolstering risk management policies to re-evaluating investment in cybersecurity after incidents, to strengthen a firm's resilience and maintain financial health (Zafar, Ko, and Osei-Bryson 2016; Gwebu, Wang, and Wang 2018; Goode et al. 2017; Akey, Lewellen, and Liskovich 2018). The literature underscores the proactive stance of managers who, cognizant of the potential for unexpected costs from security breaches, are likely to adopt strategic risk management practices. Such practices serve as a financial bulwark, aiming to shield the firm from the immediate costs of breaches and the subsequent rise in the cost of capital that heightened cyber risk entails. This perspective casts managers as forward-thinking agents of financial preparedness, actively seeking to mitigate the costs associated with cyber threats.

2.2 Cash Holdings' Role in Ex-ante Cyber Risk Management

As mentioned above, the proliferation of cyber threats poses a significant challenge to modern enterprises, not only damaging reputations and customer trust but also destabilizing core financial aspects, including sales growth and liquidity. The heightened volatility in cash flow resulting from operational disruptions, recovery costs, and the erosion of customer confidence necessitates a robust approach to working capital management.

Insights from Han and Qiu (2007) provide a crucial understanding of how firms might adjust their cash holdings in the face of such financial uncertainty. Han and Qiu (2007)'s analysis reveals that firms with limited access to external financing are more likely to bolster their liquidity to counteract the unpredictability of cash flows due to external shocks. In the context of cyber risks, this behavior translates into a heightened precautionary stance, with firms maintaining more substantial cash reserves to mitigate the financial repercussions of cyber incidents. As a matter of fact, Boasiako and O'Connor Keefe (2021) find that in their ex-post analysis, data breaches lead firms to increase cash holdings after an attack.

Han and Qiu (2007) suggest that the trade-off between hedging strategies, like cyber insurance, and the accumulation of cash reserves is a nuanced decision influenced by a firm's financial flexibility and the interplay between investment opportunities and future cash flows. As cyber threats become increasingly significant, this trade-off gains greater relevance, prompting firms to carefully weigh the relative costs and benefits of proactive cybersecurity investments against the strategic holding of liquid assets.

Hypothesis: **Firms with greater exposure to cyber threats are more likely to hold higher cash reserves as a strategic precaution ex-ante, reflecting an integrated risk management strategy that balances the use of cyber insurance with the need for liquidity to ensure operational resilience in the event of a cyber incident.**

2.3 Evolution of the Cyber Insurance Market

Despite security measures, no organization can entirely mitigate these risks. Costly data breaches averaging $9.4 million and cyber incidents have underscored the severity of the situation (Ponemon Institute LLC 2013). In response to the growing cyber threat landscape, companies began recognizing cybersecurity as a critical business risk. It introduced a shift in risk management strategies, with an increasing emphasis on risk transfer mechanisms such as insurance (Marotta et al. 2017).

Specialized cyber insurance coverage first appeared in the late 1970s, but it wasn't until 1998 that standalone cyber insurance policies emerged, thanks to the International Computer Security Association's TruSecure service (Majuca, Yurcik, and Kesan 2006). The market for these policies expanded rapidly, driven by the severe consequences of cyber events. High-profile attacks against major companies highlighted the need for financial protection against cyber threats, prompting a surge in the demand for cyber insurance and the development of more sophisticated insurance products (Josephine Wolff 2021; Nancy Gohring 2002; Orr 2021).

Regulations like California's data breach notification law in 2003, HIPAA security regulations and the EU's data protection reforms also drove the market's expansion, mandating breach disclosures and influencing global cybersecurity policies (Majuca, Yurcik, and Kesan 2006; Marotta et al. 2017). Today, the cyber insurance market offers varied coverage for different sectors, addressing first-party and third-party liabilities. While the adoption of cyber insurance has grown, concerns about coverage adequacy and cost remain.

2.3.1 Cyber Insurance : An Underdeveloped Market

Indeed, despite the significant growth of cyber risks, the cyber insurance market has been unable to keep up. The premiums in the U.S. market have expanded almost five times from $1.4 billion in 2015 to $6.5 billion in 2021 (Swiss Re Institute 2022). However, the market is still in its early stages, and it only represents 1% of the total U.S. property and casualty (P&C) insurance market (Swiss Re Institute 2022). This disparity between coverage and risk is quite noticeable; over 90% of cyber losses are not covered by insurers, which leaves businesses and individuals vulnerable to significant economic damage (NAIC Staff 2022). McAfee's 2020 report on global cybercrime costs, which was estimated at $1 trillion, further emphasizes the gap between the potential economic impact and the actual reach of current cyber insurance solutions (Smith, Lostri, and Lewis 2020).

Rapid Evolution of Cyber Threats & Lack of Historical Data: Insurers are constantly racing to keep up with the rapid development of cyber threats, a task made more difficult by the need for extensive historical data on cyber incidents (PWC 2016) . This absence of data impairs the insurers' ability to model and predict future risks with any degree of accuracy (PWC 2016; Marotta et al. 2017).

Complexity in Risk Assessment & Interdependency of Risks: The complex nature of cyber risk assessment compounds the challenge (Network and Information Security Agency 2012) . Unlike traditional insurance models with more static risks, the cyber world is dynamic, with threats that change and evolve almost daily. Insurers must grapple with the intricacies of diverse information systems and their interdependencies (Network and Information Security Agency 2012; Marotta et al. 2017) , which can result in widespread impacts from a single cyber incident.

Quantification of Losses & Regulatory Uncertainty: The financial quantification of cyber incidents is another difficulty due to intangible losses such as reputation damage, intellectual property theft, and the interruption of business services. These factors are hard to quantify and are not easily insurable (Protection and Programs Directorate U. S. Department of Homeland Security 2012; Aziz, Suhardi, and Kurnia 2020). Moreover, the regulatory landscape is still in flux, with varying laws and regulations across different regions, adding another layer of complexity for global insurance coverage.

Information Asymmetry & Cyber Risk Management Maturity: Information asymmetry further exacerbates these challenges. There is often a significant gap in what insurers know versus what the insured knows about their own cyber risks, making it challenging to develop policies that are both comprehensive and fair (Aziz, Suhardi, and Kurnia 2020; Marotta et al. 2017; Bailey 2014). Additionally, many organizations still need to reach a level of cyber risk management maturity that insurers find adequate for risk assessment purposes (Bailey 2014).

Capacity and Reinsurance Challenges & Catastrophe events : Capacity limitations within the insurance market, coupled with a still-maturing reinsurance sector for cyber risks, mean that insurers have limited options to offload risk, leading to constraints on the amount of risk they can underwrite (Eling, McShane, and Nguyen 2021). This situation is made worse by the potential for loss aggregation due to widespread vulnerabilities that could trigger simultaneous large-scale attacks. With heightened geopolitical tensions, mainly due to the war in Ukraine and US-China relations, there is an elevated risk of state-sponsored cyberattacks that could have catastrophic fallout on a global scale (Kevin Collier 2023).

Premium Pricing Challenges: Pricing premiums appropriately is also a persistent hurdle. Insurers must balance the need to set premiums that accurately reflect the risk while ensuring that the insurance remains affordable for customers. This is made difficult by the fast pace of change in the cyber threat landscape and the diverse nature of potential incidents (Aziz, Suhardi, and Kurnia 2020 ; Marotta et al. 2017) .

Coverage Limitations and Exclusions & Silent Cyber Issues : Insurance policies themselves often have many limitations and exclusions, which can leave policyholders with gaps in coverage (Aziz, Suhardi, and Kurnia 2020 ; Marotta et al. 2017). The issue of non-affirmative or "silent" cyber risks remains unresolved, as traditional policies do not always clearly delineate their coverage of cyber incidents.

Hypothesis: **Firms that face greater exposure to cyber threats are more likely to purchase cyber insurance, but the issuer will need help assessing the true risk.**

3 Data

3.1 SecurityScorecard

This study uses cybersecurity data from SecurityScorecard from actual monitoring of firms, including daily data from SP1500 companies between October 2022 and October 2023. This allows for quarterly analysis. SecurityScorecard provides a comprehensive cybersecurity posture assessment of an organization. This assessment is represented by a Total Score, which is a letter grade ranging from A (90-100) to F (below 60), making it easy to understand. The Total Score is calculated by taking a weighted average of 10 Factor Scores, each of which represents a different aspect of cyber risk. These Factor Scores are derived from various cybersecurity signals that are categorized into ten risk factor groups. Each issue within a group is assigned a severity-based weight, except for informational and positive issues that, while reported for awareness, do not affect the score (Sohval 2023).

1. **Network Security**: Checks for risky or unsecured network ports through public data.
2. **DNS Health**: Evaluates an organization's DNS setup and historical security incidents.
3. **Patching Cadence**: Assesses how promptly an organization installs security patches.
4. **Endpoint Security**: Monitors potential security gaps based on software and plugin metadata.
5. **IP Reputation**: Uses various intelligence sources to assess the risk associated with an

organization's IP addresses.

6. **Application Security**: Analyzes known security weaknesses reported in various online databases.
7. **Cubit Score**: Evaluates diverse security concerns, including the reputation of an organization's IP addresses.
8. **Hacker Chatter**: Gathers and interprets data from covert online spaces frequented by hackers.
9. **Information Leak**: Looks for signs of exposed sensitive information in hacker discussions.
10. **Social Engineering**: Gauges an organization's risk of falling victim to manipulative tactics aimed at breaching security.

To ensure that the Total Score correlates strongly with the likelihood of a breach, SecurityScorecard uses machine learning to optimize the weights of these risk factors. Companies rated F are 13.8 times more likely to suffer a breach than those rated A, according to statistical analysis.

3.2 Data Breaches

In the fields of finance, accounting, and information systems, the Privacy Right Clearinghouse dataset has been extensively used in prior research. However, some researchers have pointed out that the dataset overlooks low economic magnitude breaches and disregards critical attacks like website defacements and DDoS attacks (Francis, Hu, and Shohfi 2021). Abbiati et al. (2021) noted that commercial datasets on cyber incidents provide more than 15,000 observations for a sample period from 2005 to 2018, compared to non-profit databases such as the Breach Level Index (BLI), the Identity Thief Resources Center (ITRC), Data Loss DB, and the Privacy Right Clearinghouse (PRC), which contain each less than 10,000 incidents. To create a comparable database to commercial ones, Abbiati et al. (2021) combined the abovementioned databases.

Therefore, I have combined the aforementioned datasets in this research. First, I compiled over 10,000 data breaches from the Identity Thief Resources Center databases between 2005 and 2019, which are no longer freely accessible to the public. In 2020, they started charging for access to their data. Then, I added over 9,000 observations from the Privacy Right Clearinghouse from 2005 to 2018, along with data from the data loss DB dataset, which has data from 2000. Next, I added over 7000 data breach cases from the Breach Level Index, which is presently inaccessible and spans 2013 to 2017, and focused on U.S. public companies. I extracted publicly traded companies from each dataset, combined the information, and removed duplicates. I discovered almost 1800 breaches between 2000 and 2019. Some firms experience multiple breaches each year, which are considered a single incident for the year in question. Additionally, the maximum severity of the breach, as measured by the amount of stolen records, will be recorded for repeating breaches within the same year. In this research, I do not limit the dataset to external attacks only, which are much more extensive than the previous dataset disclosed in the literature, but also include inside breaches.

Nevertheless, for this research, I will restrict the sample period to after 2005 because no state breach notification laws compelled corporations to report their breaches before 2000. Therefore, there could be many unreported breaches. This is another reason why the cyber breach datasets are heavily biased because several old breaches were announced by news, not by the firms, which have an apparent reason to be reluctant to provide information. Moreover, I have excluded all financial and utility companies, i.e., those with Standard Industrial Classification (SIC) codes 6000–6999 or 4900–4999, because they are required to meet statutory capital requirements and may be subject to regulatory oversight in some states. Additionally, I eliminated observations with negative or missing total book assets and substituted missing values in R&D with zeros. The data, as mentioned earlier, was matched with COMPUSTAT and CRSP.

3.3 Measures of Cyber Risk

3.3.1 SecurityScorecard Score

The Raw Factor Score (RFS) is determined by adding together the products of the severity-based weights and the standard scores (z-scores) for each issue within a factor, such as Network Security, DNS Health etc. The RFS for a domain of a company is the sum of these calculations for all issues within a factor, where the severity-based weight reflects the importance of an issue and the z-score indicates how much the issue deviates from the mean in standard deviation units. Informational or non-negative issues are assigned a weight of zero and don't affect the score. These raw scores are then scaled to range from 0 to 100.

Raw Factor Score:

$$RFS_d = \sum_{i \in f} w_i \times z_{di}$$

The weighted sum of the issue-level z-scores is used to compute where (RFS_d) is the raw factor score for domain (d), (w_i) is the severity-based weight for issue (i), and (z_{di}) is the z-score for domain (d) and issue (i). The sum is calculated over all issues (i) in factor (f).

The Total Score is the weighted average of scaled factor scores, emphasizing weaker areas to reflect the principle that security is only as robust as its weakest component. This means that lower factor scores disproportionately lower the Total Score, highlighting areas of significant risk.

Total Score:

$$TS_d = \frac{\sum_f w_f \times g(FS_{df}) \times FS_{df}}{\sum_f w_f \times g(FS_{df})}$$

Finally, the Total Score is calculated as the weighted average of the individual factor scores, where (TS_d) is the total score for domain (d), (w_f) is the severity-based weight of factor (f), (FS_{df}) is the factor score for domain (d) and factor (f), and $(g(\cdot))$ is a non-linear weighting function which gives greater emphasis to low factor scores.

Scores are updated daily, and to make the risk interpretation more intuitive, they are transformed so that higher scores indicate higher risk and lower scores indicate lower risk. This is done by subtracting the SecurityScorecard Score from one more than the maximum score observed, effectively reversing the scale for easier understanding.

To allow for a better interpretation and comparison with other measure in the analysis, the variable has been transformed so that when the score increase, the risk is higher, and when the score decrease, the cyber risk is lower.

The transformation is Security Score = Max(SecurityScorecard Score)+1−SecurityScorecard Score, it allows to have the same variation but the only thing that changes is the ability to have an easier intepreation.

3.3.2 Cybersecurity Risk Score (10-K measure)

Several research works have aimed to overcome the constraints of ex-post evidence by scrutinizing firms' cybersecurity disclosure practices, drawing insights from their 10-K filings (Florackis et al. 2022; Lattanzio and Ma 2023; Jamilov, Rey, and Tahoun 2021). These studies employ textual analysis methodologies to evaluate a firm's cybersecurity stance.

In alignment with this body of literature, I have devised a measure rooted in 10-K disclosures. This construction is orchestrated utilizing a sophisticated dictionary, which mirrors the comprehensive lexicon developed by Lattanzio. It encapsulates terms curated by the NICCS, alongside phrases incorporated from Gordon et al. (2010). A detailed presentation of the utilized vocabulary is articulated in the appendix.

Following the methodology of Loughran and Mcdonald (2011) , each term within our dictionary is assigned a weighted value, adhering to a specific algorithm. Here, $W_{i,j}$ signifies the weight allotted to term i in document j, N symbolizes the cumulative count of 10-Ks in the sample, df_i denotes the number of documents marked by the presence of term i, and $tf_{i,j}$ represents the unadjusted count of word i in document j, while a_j is indicative of the average word frequency in the document.

$$w_{i,j} = \begin{cases} \frac{(1+\log(tf_{i,j}))}{(1+\log(\alpha_j))} \log \frac{N}{df_i} & \text{if } tf_i \geq 1 \\ 0 & \end{cases}$$

Loughran and Mcdonald (2011) elaborated that the initial term minimizes the influence of high-frequency words through a logarithmic transformation, whereas the subsequent term adjusts for the prevailing commonality of a specified term. Noteworthy is the decision to abstain from logging the weighted word frequency. However, the log measure also provides findings similar to the core results, speaking to the robustness of the results.

3.3.3 Probability of Breach

In an effort to quantify the anticipated cyber risk, represented as the ex-ante probability of future breaches, a logistic regression model is employed within a dynamic, expanding window framework. This model leverages historical data of previous breaches to estimate a firm's likelihood of experiencing a breach. The logistic regression is conducted as follows :

$$\text{Prob}(\text{Breach}_{i,k,t}) = \alpha_0 + \alpha_1 \text{Previous breach dummy}_{it-1} + \alpha' X_{i,k,t-1} + \text{ Industry}_k + \text{Year}_t + \varepsilon_{i,k,t}$$

In this equation, (i), (k), and (t) denote the firm, industry, and year respectively. The **'Previous breach dummy'** variable is set to one if a firm has previously encountered at least one breach.

For validation and robustness, it should be noted that various breach measures, such as the total number of breaches or the occurrence of multiple breaches, were also applied in the analysis. Importantly, these alternative approaches did not deviate significantly from the primary findings of the study.

3.4 Data Summary

3.4.1 Securityscorecard dataset

The base data set underpinning this analysis was procured from SecurityScorecard, covering the period from October 2022 to October 2023. It comprises daily data on the overall cybersecurity risk score for each firm, in addition to specific factors like network security and DNS health. These scores were aggregated on a quarterly basis and then combined with financial data from Compustat and CRSP, providing a comprehensive view of firms' cybersecurity and financial positions.

Upon a thorough examination, several key patterns emerge from the dataset:

Cash Holdings: On average, firms held 12% of their total assets as cash, indicating a cautious approach to liquidity management. However, this average masks significant variability, as evidenced by a standard deviation of 13.4% and a maximum cash holding of 75%. Such variation reflects diverse financial strategies across firms: while some prefer to keep a large liquidity buffer, others may have varying reasons for lower cash holdings, such as challenges in cash flow management or high levels of receivables.

Security Score: The average cybersecurity score was 19.143% of total assets, with notable variations (standard deviation of 9.46). The data also showed skewness towards higher values, peaking at 64.022%. This implies a broad spectrum of cybersecurity preparedness among firms, with some maintaining high security levels while others lag behind.

Operational Expenditures: The analysis of operational expenditures revealed that SG&A and R&D expenses, relative to sales, accounted for 4.6% and 7.5% of assets, respectively. These figures illustrate the different priorities firms have in terms of operational efficiency and investment in innovation. The allocation to SG&A and R&D provides insight into how firms balance day-to-day administrative costs against longer-term research and development endeavors.

3.4.2 Data breach dataset

After merging the different datasets, I carefully excised all missing variables for each variable included in the analysis, followed by a winsorization at 1% by year. The sample period covers 2005 to 2018. Before initiating the analysis, these essential steps were taken to meticulously scrutinize the distribution of the dependent and primary variables of interest.

In considering **"Probability Breach,"** the dataset unveils illuminating findings. It depicts that the average likelihood of cybersecurity breaches across firms stands at a mean of 2%, complemented by a 5% standard deviation. It suggests that the ensemble of companies predominantly faces a low probability of encountering cybersecurity breaches. However, it's pivotal to discern that there exists a segment of firms susceptible to high risk, manifested by a max value that unveils a 41.7% probability of a breach occurrence.

Shifting focus towards **Oyima (2023)** provides an index that reveals significant insights into firms' cybersecurity preparedness. The data, with an average score of 1.418 and a substantial standard deviation of 1.952, reaching an exceptional 11.996 peak, portrays a landscape of varied cybersecurity postures. It signifies that a predominant cluster of companies exhibits a median level of cybersecurity risk, disturbed with a few outliers that manifest remarkedly elevated risk profiles. This spectrum of results underscores cybersecurity's paramount importance and inherent variability.

3.4.3 Skewness of Dependent Variables

Traditional corporate finance research often centers on estimating the conditional mean of skewed dependent variables given a set of predictors, typically employing linear regression methods. However, this approach, as highlighted by (Kieschnick, Rotenberg, and Song 2023), has problems as linear regressions on skewed dependent variables produce biased estimates of the coefficients and their standard errors.

As Figure 2 demonstrates, a firm's cash holdings are highly skewed. Therefore, in this study, I use their recommended quantile regression approach to assess firms' ex-ante cyber risk impact on risk management and financing pre-breach. This approach offers a more accurate and comprehensive understanding of the relationships as it considers the entire distribution of the dependent variable, not just the mean. This treatment is especially valuable for investigating the potential heterogeneity in treatment effects.

4 Empirical Strategy

While I primarily employ a quantile regression approach, I will also utilize the conventional conditional mean approach to address the concerns of those wanting a more traditional approach.

My analyses are focused on firms' behavior before a cyber breach. The regression analysis leverages ex-ante cyber risk indicators, specifically the cyber risk score established earlier and the probability of a breach as a secondary measure. To ensure rigorous control over potential confounding factors, I incorporate industry and year-fixed effects, following established practices outlined in the literature, particularly in Floråckis et al. 2022. Robust standard errors are clustered at the firm level to account for potential within-firm correlation.

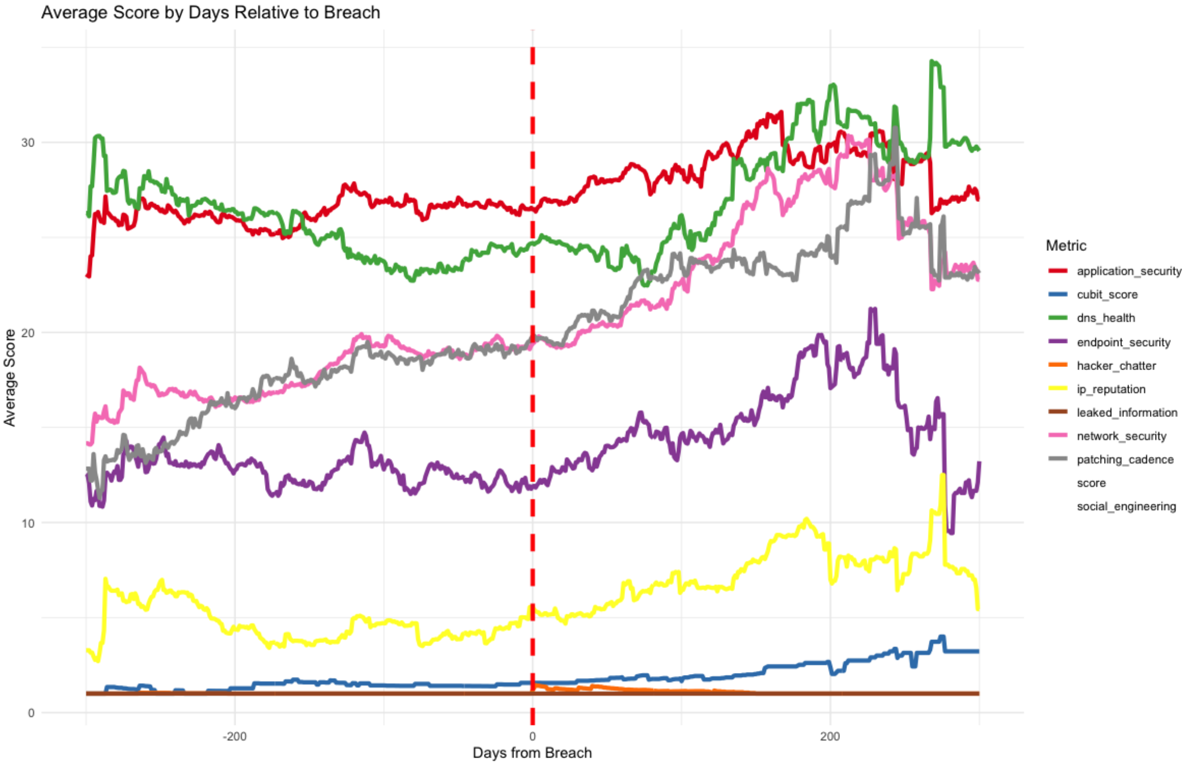
Additionally, I include controls for firm size, growth opportunities (Tobin's q), profit margin, and sales growth to account for firms' visibility and profitability variations, factors that may influence cyber breaches. The analysis also incorporates variables related to research and development, as it may determine a firm's susceptibility to breaches. Moreover, capital expenditures, which reflect a firm's infrastructure and asset tangibility, potentially indicative of digital sophistication, are included as controls, given their potential impact on the variable of interest and overall cybersecurity risk profile. Table 1 provides their summary statistics.

Thus, my basic empirical model is as follows:

$$Q_\tau(Y|\ Ex - ante\ cyber\ risk, X, Industry_k, Yeart_t) =$$
$$\alpha + X'\beta + \gamma\ Ex - ante\ cyber\ risk + \Delta$$

5 Discussion

5.1 Firms' behavior prior to a cyber incident

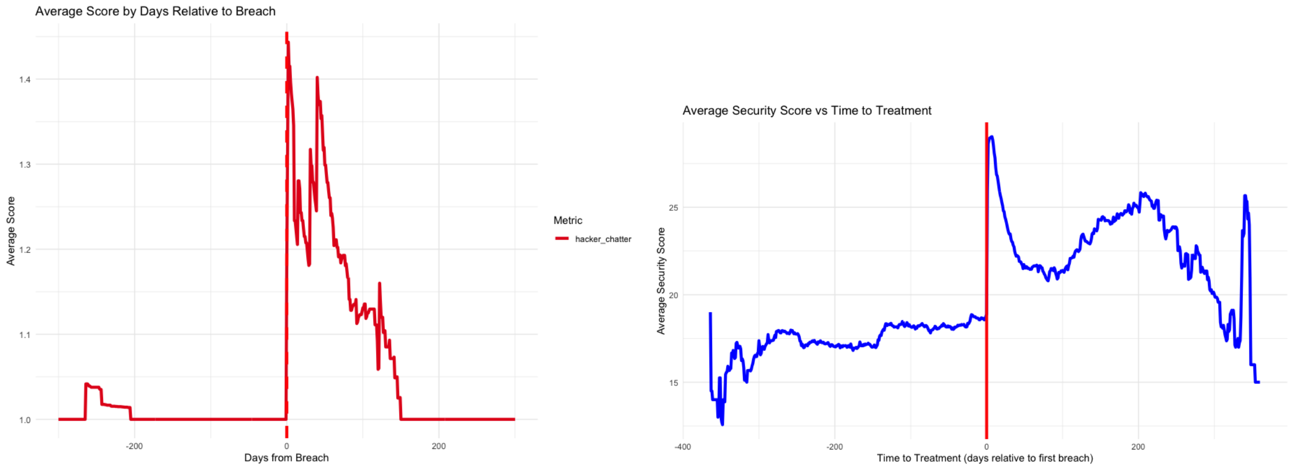


This graph displays the average security score for all the SP1500 firms. It allows us to show the average score for different aspects of cyber security factors from securityscorecard. Each score was transformed for a more straightforward interpretation, as detailed in the data section.

As we delve into the anticipatory behavior of firms regarding cyber risks, it's crucial to examine the visual data presented, which depicts the cyber risk metrics for SP1500 firms before and after a breach. This evidence plays a pivotal role in reshaping the ongoing debate in finance literature about the unpredictability of breaches. Contrary to the notion of breaches being entirely unforeseen, the graph clearly illustrates a noticeable escalation in cyber risk factor scores in the months leading up to a breach.

This trend is significant, especially considering that some companies actively monitor these security scores, allowing their IT departments to strategize accordingly. Around nine months prior to an attack, we observe an uptick in hacker activity and a growing risk due to delayed patching. While several risk factors show an increase, the persistent issue of unaddressed patching and network security is particularly alarming.

Recent reports indicate that approximately 60% of data breaches in the past two years were due to unpatched operating systems and applications. This vulnerability, often a result of subpar patch management, is particularly costly in terms of downtime and disruptions, especially for



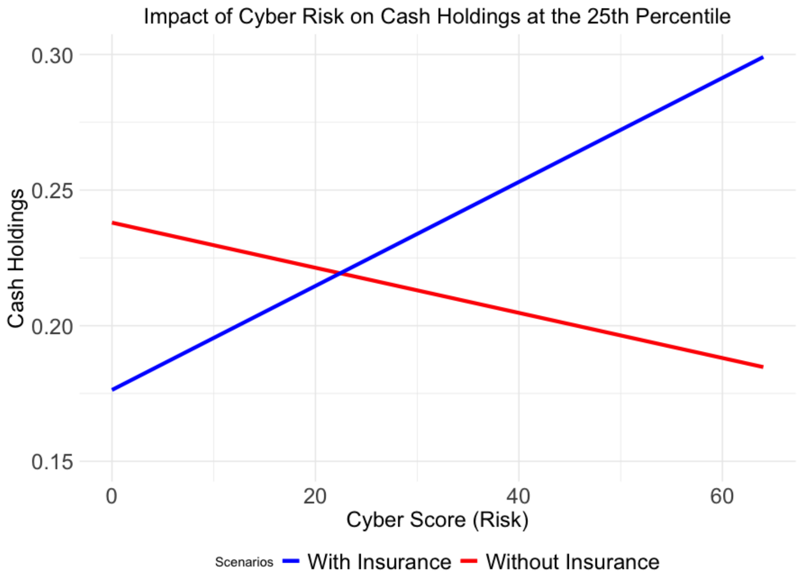
The graph on the left shows the average hacker chat scores for the SP1500 firms from October 2022 to October 2023, while the graph on the right displays the overall scores from Securityscorecard

larger organizations (Sheridan 2020). The urgency of effective patch management has been further amplified by the rapid transition to remote work environments amid the COVID-19 pandemic (Sheridan 2020). While patching incurs significant costs, the financial impact of disruptions and operational downtime for larger companies can be even more substantial, underscoring the need for timely and effective patch management strategies. These insights underscore the crucial need for a deeper understanding of firms' preparatory actions in the face of impending cyber threats.

5.2 Ex-ante analysis on Cash Holdings

I begin my analysis by examining the complex relationship between cyber insurance and cash management within corporate risk management strategies. The evidence in Table 2 suggests that the use of cyber insurance markedly diminishes the necessity for firms to hold large cash reserves against possible cyber breaches. The data shows a reduction in cash holdings by 0.05, which is approximately 41% of the average cash holdings, quantified at 0.127. This significant decrease highlights the impactful role of cyber insurance in bolstering financial flexibility for firms. By reducing the need for extensive cash reserves, cyber insurance allows companies to more effectively manage and minimize the costs tied to maintaining high levels of liquidity. Such an observation underscores the importance of cyber insurance as a tool for mitigating cyber-related costs.

Yet, an unexpected pattern emerges among firms facing heightened cyber risks. Despite having cyber insurance, these firms are observed to increase their cash reserves. This behavior contrasts with firms lacking cyber insurance, which generally do not increase — and in some cases, as per the 25th percentile, even decrease — their cash holdings. This dichotomy suggests that even with the risk mitigation provided by cyber insurance, firms with greater exposure to cyber threats may still perceive a need for additional financial preparedness, opting to retain more substantial cash reserves as a precautionary measure.



The graph provides a graphical representation of the results presented in Table 2 for the second column, which shows the analysis at the 25^{th} percentile.

This pattern suggests that firms with cyber insurance may adopt a more risk-averse stance, accumulating cash as an additional safeguard against potential breaches. On the other hand, firms without cyber insurance, potentially due to constraints in the cyber insurance market such as limited availability and high premiums, might be channeling their resources towards enhancing cyber defenses instead. This behavior could be a strategic decision, particularly considering that cyber insurance policies often have coverage limitations and may not fully encompass all aspects of breach-related losses.

Therefore, while cyber insurance is undeniably a critical component of risk management, it's essential to view it within the broader context of a firm's overall cybersecurity strategy. The decision to invest in cyber insurance or to allocate resources to other forms of cyber protection should be seen as part of a comprehensive approach to managing cyber risks, influenced by market dynamics and the specific risk profile of each firm.

5.3 Ex-ante analysis on IT expenses

In light of the earlier discussion on firms' increasing cash reserves in the face of cyber threats, particularly those with cyber insurance, we now turn our attention to another aspect of their risk management strategies: IT investments. This shift in focus is crucial to understand whether firms are complementing their insurance coverage with adequate investment in cyber defenses or relying solely on insurance as their primary safeguard.

Despite the intuitive expectation that firms averse to cyber risks would proportionately increase their IT expenditures, the evidence from Tables 3 and 4 presents a different narrative. They reveals that firms with cyber insurance are not significantly ramping up their IT investments, typically accounted for in SG&A and R&D expenses[1]. This finding suggests a potential reliance on insurance policies over direct investment in cybersecurity infrastructure, contrasting the behavior of firms without such insurance.

Contrastingly, in the 25th quantile of firms without cyber insurance, there is a noticeable increase in IT investment, as indicated by higher SG&A and R&D spending. This pattern suggests that these firms are proactively enhancing their cyber defenses, as opposed to those with cyber insurance who appear to rely more on their insurance coverage.

This leads to a hypothesis of moral hazard: firms with cyber insurance might not feel the same urgency to upgrade their IT infrastructure, relying instead on their insurance policies. Yet, a critical question arises: why do firms with cyber insurance not increase their cash holdings despite the heightened risk? The answer lies in the inherent frictions within the cyber insurance market.

Cyber insurance policies, while crucial in managing cyber risks, often come with significant limitations and exclusions. This issue has become increasingly evident with the evolution of cyber threats. The COVID-19 pandemic, for instance, saw a surge in ransomware attacks and more sophisticated cyber threats, prompting insurers to revise their policy terms. Caspar Stops, head of cyber at Optio, highlights this shift: many organizations found ransomware explicitly excluded from their policies, leading to 74% experiencing increased premiums, 43% seeing higher deductibles, and 10% facing reduced coverage benefits (Cohn 2021). These adjustments by insurers reflect their response to the dynamic cyber risk landscape, influencing how firms approach and manage their risk.

A notable instance that underscores the complexities of cyber insurance is the case of the NotPetya attacks. When Mondelez and pharmaceutical giant Merck faced significant damages from these attacks, they turned to their insurers for compensation. Despite having ***'property insurance'*** policies, both companies encountered challenges due to the ***'war exclusion'*** clause. Merck's claim of $1.4 billion against Ace American Insurance Co. and Mondelez's $100 million claim against Zurich American Insurance Company were initially rejected, with insurers citing the attacks as acts of war, thereby falling outside the policy coverage (alliance 2023).

However, the outcome of Merck's lawsuit in the New Jersey Superior Court provided a pivotal moment in cyber insurance jurisprudence. The court ruled that the damages caused by NotPetya did not constitute an act of war, as there were no formal war declarations or involvement of armed soldiers (Andrea Vittorio 2022). This ruling in favor of Merck highlights a critical aspect of cyber insurance: the interpretation of policy clauses can significantly impact the indemnification process,

[1] It's important to note that the assessment of IT investments in financial reports is challenging due to the lack of explicit disclosure. IT expenditures are often embedded within SG&A expenses, making them difficult to isolate. Consequently, I follow prior researchers, and use SG&A and R&D expenses as proxies for IT investments (Lim et al. 2011; Khallaf 2012) .

especially in cases where cyber incidents intersect with geopolitical events.

These examples underscore the challenges that firms face in seeking comprehensive and reliable cyber insurance coverage. The evolving nature of cyber threats and the complexities of policy terms necessitate a deeper understanding of how cyber insurance functions in practice and its limitations as a risk management tool.

Moreover, the challenge in quantifying losses, especially intangible ones like reputational damage, complicates the insurance equation (Aziz, Suhardi, and Kurnia 2020). This situation often results in firms not receiving full indemnification for their losses, further affecting their decision-making regarding cash reserves and IT investments.

5.4 A Potential Moral Hazard in the Cyber Insurance Market

Building on the earlier discussion, we now delve deeper into the potential moral hazard issues associated with cyber insurance. The challenge of directly measuring cyber investments through accounting methods limits the strength of the evidence I can gather. However, if a lack of investment in cyber defenses translates to a higher incidence of breaches, this relationship should be observable in the data.

The logistic regression analysis in table 5, examining the correlation between firms' cybersecurity scores, their cyber insurance holdings, and the occurrence of breaches, yields significant findings. Interestingly, firms with cyber insurance are more likely to experience breaches. This correlation does not imply causation; cyber insurance itself does not lead to breaches. Yet, it aligns with our earlier discussion suggesting that firms with cyber insurance might become complacent in their cybersecurity efforts, inadvertently exposing themselves to higher risks.

This leads to a critical question: Why would firms take such risks, especially given the understanding that cyber insurance is not a foolproof safeguard against breaches (NAIC Staff 2022) ? The answer may lie in the relative cost-benefit analysis these firms conduct. For companies that can afford cyber insurance, the cost of maintaining extensive cybersecurity measures might outweigh the perceived benefits, particularly when the financial impact of breaches is relatively low compared to their overall revenue and size (Michael Kassner 2015). Faced with this scenario, some firms might opt to hedge their risk through a combination of cyber insurance and cash reserves, rather than investing heavily in cybersecurity infrastructure.

The evidence in Table 6[2] provides additional insights into this issue. This table focuses on the

[2] It is important to mention that this analysis excludes financial firms due to their unique regulatory environment. Additionally, the dataset used in this study extends only up to 2019. Therefore, the landscape and market perceptions might have evolved since then, especially if cyber insurance providers have implemented more stringent reforms, as suggested by various recent articles. These evolving dynamics in the cyber insurance market and their impact on firms' risk management strategies remain an area ripe for future research.

unexpected scope negatives, representing the instances where the severity of a firm's current breach (measured as the Total Number of Records Stolen relative to sales) exceeds the average severity of past breaches. The data reveals a striking pattern: when a firm's breach severity surpasses market expectations, there is a consequent negative reaction in the stock market. This indicates that the market penalizes firms for breaches that are more severe than anticipated.

What's particularly notable is the amplified negative response from the market for firms that hold cyber insurance. This raises two possible interpretations. First, it might suggest that firms with cyber insurance have weaker cyber defenses, leading to more severe breaches and thus a stronger market backlash. Alternatively, it could imply that the market perceives these firms as overly reliant on their insurance policies instead of investing adequately in cybersecurity, and reacts negatively to this perceived complacency.

5.5 Reframing Cyber Security: Understanding the Flaws in Current Approaches

The analysis suggests a complex relationship between cyber insurance and corporate cybersecurity strategies. The current approach to cyber risk analysis typically revolves around two key parameters (Marotta et al. 2017): the probability of an incident and its potential impact, conceptualized as :

$$\textbf{Risk} = \textbf{Probability} \times \textbf{Impact}$$

While cyber insurance plays a crucial role in mitigating the financial impact of breaches, it primarily addresses the aftermath, not the prevention. This is evident in the way cyber insurance is often structured, focusing more on the impact rather than the probability of cyber incidents.

In delving deeper into the interplay between cyber insurance and cyber risk management, it's important to consider the criteria set by insurers. While cyber insurance does impact the probability aspect of cyber risk by imposing specific security requirements, these prerequisites often fall short of comprehensive risk assessment. As highlighted in Romanosky et al. (2019) 's study, insurers tend to gather only basic information about a firm's technology and infrastructure. This typically includes queries about the number of computing devices, IP addresses, or website URLs, which provide a rudimentary view of the insured entity's cybersecurity landscape.

This surface-level evaluation of cyber risk by insurers raises concerns about the accuracy and depth of risk assessment. Such an approach can lead to a significant gap between a firm's cybersecurity posture and what the insurer perceives. Notably, it often overlooks intricate aspects like the security measures of third-party vendors, which, as evidenced by numerous data breaches, are a critical vector of cyber threats (Verizon 2022). Consequently, this disconnect can result in firms with cyber insurance policies having a false sense of security, believing themselves to be adequately protected based on minimal compliance with insurance requirements.

On the flip side, investing in cyber defenses impacts both the likelihood and consequences of cyber incidents. However, the challenge lies in quantifying the return on investment for cybersecurity measures. As Alex Blau (2019) notes, determining the ROI of cybersecurity investments is fraught with uncertainty, given the ever-changing digital threat landscape. This difficulty is compounded by common cognitive biases in decision-making. Many managers view cybersecurity as a static target that can be 'solved' with enough one-shot investment, neglecting the reality that it's an ongoing process requiring continual adaptation.

Moreover, behavioral economics highlights how human judgment, often relied upon in the absence of concrete data, can be flawed. Decision-makers may underestimate the necessity of continuous investment in cybersecurity, falsely equating a lack of breaches with effective security, or over-relying on compliance with standards like NIST or FISMA as adequate protection.

Therefore, a reevaluation of cybersecurity strategies is imperative. Firms should not perceive cybersecurity as a one-time investment or a problem that can be fully outsourced to insurance. Instead, they must adopt a more holistic approach combining robust cyber defenses with cyber insurance, continuously adapting to the evolving threat landscape. This integrated strategy is not just about mitigating risks post-breach but also about reducing the likelihood of breaches in the first place, thus safeguarding both tangible and intangible assets, such as reputation and trust, that are not insurable.

6 Conclusion

The landscape of cybersecurity in the corporate world is complex. Prior research often ignores that firms frequently exhibit anticipatory behavior. This behavior is consistent with the discernible patterns in security scores before breaches. This insight alone compels a consideration of how firms mitigate the costs of a data breach prior to an attack. I identify three main ways firms might mitigate the ex-post costs of a data breach: (1) investing in internal cybersecurity controls, (2) adjusting the firm's financial posture, and (3) buying cyber insurance.

The interaction between cyber insurance and corporate financial strategies, particularly regarding cash holdings, uncovers a nuanced dynamic. While cyber insurance provides a degree of financial cushioning against breaches, it is not a panacea. Firms holding cyber insurance are paradoxically found to be increasing their cash reserves, suggesting that these are more complementary than substitutive. However, this raises a concern: the potential moral hazard of cyber insurance, where firms might rely on their policies at the expense of essential investments in IT security. This tendency not only exposes firms to heightened risks but also questions the adequacy of their risk management frameworks.

The key points of this study are that managers anticipate the potential for data breaches, but appear to put more emphasis on adjusting their financial posture and buying cyber insurance to mitigate their associated ex-post costs.

7 Tables

Table 1: The following table summarizes the variables utilized in the upcoming analysis, which will be conducted quarterly for fiscal years 2022 and 2023, where the data is available for security scorecard scores. The indicator variable represents cyber insurance in a firm's 10-K documents. It is assigned a value of 1 when terms related to cyber insurance are mentioned, determined by the presence of National Initiative for Cybersecurity Careers and Studies (NICCS) keywords within ten words before or after the word "insurance" in the 10-K documents. Additionally, the variable takes the value of 1 when firms explicitly state in their 10-Ks that they have cyber insurance. The other variables being assessed in this context include Size, Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capex, Asset Tangibility, R&D, and Probability of Breach : Firm Age (defined as the log of the firm's age), Firm Size (defined as the log of total assets), Sales Growth (defined as the change in sales from the previous period: $(sale_t/(sale_{t-1} - 1)))$, Profit Margin (defined as EBITDA over total assets: $ebitda/at$), Capital Expenditures (defined as capital expenditure over property, plant, and equipment: $capx/ppent$), Tobin's Q (defined as adjusted assets over total assets: $(at - ceq + (prcc_f \times csho))/(at))$, Leverage (defined as long term debt over total assets: $dltt/at$), Asset Tangibility (defined as the ratio of tangible assets to total assets), R&D Expenditures (defined as R&D over total assets: xrd/at). The dependent variables - Receivables, Inventory, Payables, Notes Payables, Repurchases, and Cash Holdings ratios - are computed by dividing the respective balance sheet or income statement item of the next period (lagged one period) by the total assets of the current period.

	mean	sd	min	max
Security Score	19.143	9.146	1.000	64.022
Cyber Insurance	0.350	0.477	0.000	1.000
Cash	0.127	0.134	0.000	0.794
Size	8.281	1.256	5.711	11.460
Age	3.315	0.659	1.609	4.304
Tobin's Q	2.255	1.593	0.771	9.479
Leverage	0.274	0.176	0.001	0.785
Profit Margin	0.018	0.023	-0.066	0.109
Sales Growth	-0.007	0.138	-0.603	0.516
Capex	0.098	0.080	0.000	0.463
Asset Tangibility	0.241	0.209	0.001	0.882
R&D(scaled by PPENT)	0.075	0.173	0.000	1.064
SG&A$_{sales}$	0.046	0.037	0.001	0.197
R&D$_{sales}$	0.044	0.077	0.000	0.391
Observations	1379			

Table 2: This table presents regressions for firms that have not yet experienced a data breach and are subjected to potential future cyber breaches. The primary variable of interest is the securityscorecard, the transformed variable from the securityscorecard score as detailed in the data sections. The control and primary variables are all lagged by one period, including Size, Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capex, Asset Tangibility, R&D, and Probability of Breach. Firm Age is defined as the natural logarithm of the firm's Age, and Firm Size is defined as the natural logarithm of total assets. Sales Growth is defined as the change in sales from the previous period: $(sale_t/(sale_{t-1} - 1))$, Profit Margin is defined as EBITDA over total assets: $ebitda/at$, Capital Expenditures is defined as capital expenditure over property, plant, and equipment: $capx/ppent$, Tobin's Q is defined as adjusted assets over total assets: $(at - ceq + (prcc_f \times csho))/at$, Leverage is defined as long-term debt over total assets: $dltt/at$, Asset Tangibility is defined as the ratio of tangible assets to total assets, and R&D Expenditures is defined as R&D over total assets: xrd/at. The significance levels are denoted by * for $p < 0.1$, ** for $p < 0.05$, and *** for $p < 0.01$

regressions analysis

	(1)	(2)	(3)	(4)
VARIABLES	Cash	Cash	Cash	Cash
Security Score	-0.000366	-0.000832**	-0.000474	6.15e-05
	(0.000537)	(0.000393)	(0.000477)	(0.000744)
Cyber Insurance	-0.0515**	-0.0617***	-0.0539***	-0.0422
	(0.0208)	(0.0159)	(0.0186)	(0.0281)
Security Score × Cyber Insurance	0.00208**	0.00275***	0.00224***	0.00147
	(0.000948)	(0.000700)	(0.000845)	(0.00130)
Size	-0.0188***	-0.00938***	-0.0166***	-0.0274***
	(0.00369)	(0.00280)	(0.00335)	(0.00508)
Age	-0.0243***	-0.0189***	-0.0230***	-0.0292***
	(0.00658)	(0.00526)	(0.00598)	(0.00857)
Tobin's Q	0.0185***	0.0118***	0.0169***	0.0246***
	(0.00396)	(0.00344)	(0.00368)	(0.00498)
Leverage	-0.174***	-0.140***	-0.166***	-0.206***
	(0.0305)	(0.0213)	(0.0270)	(0.0431)
Profit Margin	-0.245	-0.0838	-0.207	-0.392
	(0.226)	(0.154)	(0.199)	(0.316)
Sales Growth	-0.0196	0.00596	-0.0136	-0.0430
	(0.0266)	(0.0185)	(0.0235)	(0.0369)
Capex	0.0742	0.0125	0.0598	0.131
	(0.0680)	(0.0497)	(0.0609)	(0.0921)
Asset Tangibility	-0.0924***	-0.0708***	-0.0873***	-0.112***
	(0.0272)	(0.0210)	(0.0244)	(0.0365)
R&D	0.204***	0.154***	0.192***	0.250***
	(0.0319)	(0.0311)	(0.0305)	(0.0374)
Constant	0.382***	0.238***	0.349***	0.515***
	(0.0408)	(0.0310)	(0.0372)	(0.0566)
Observations	1,354	1,354	1,354	1,354
R-squared	0.480			
Regression Type	OLS	Quantile	Quantile	Quantile
Quantileth	None	25	50	75
Industry fixed effects	Yes	Yes	Yes	Yes
Year-Quarter fixed effects	Yes	Yes	Yes	Yes

Robust Clustered standard errors at firm level in parentheses

*** $p<0.01$, ** $p<0.05$, * $p<0.1$

Table 3: This table presents regressions on SG&A$_{sales}$, defined as SG&A to Sales, for firms that have yet to experience a data breach and are subjected to potential future breaches. The primary variable of interest is the securityscorecard, the transformed variable from the securityscorecard score as detailed in the data sections. The control and primary variables are all lagged by one period, including Size, Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capex, Asset Tangibility, R&D, and Probability of Breach. Firm Age is defined as the natural logarithm of the firm's Age, and Firm Size is defined as the natural logarithm of total assets. Sales Growth is defined as the change in sales from the previous period: $(sale_t/(sale_{t-1} - 1))$, Profit Margin is defined as EBITDA over total assets: $ebitda/at$, Capital Expenditures is defined as capital expenditure over property, plant, and equipment: $capx/ppent$, Tobin's Q is defined as adjusted assets over total assets: $(at - ceq + (prcc_f \times csho))/at$, Leverage is defined as long-term debt over total assets: $dltt/at$, Asset Tangibility is defined as the ratio of tangible assets to total assets, and R&D Expenditures is defined as R&D over total assets: xrd/at. The significance levels are denoted by * for p < 0.1, ** for p < 0.05, and *** for p < 0.01

regressions analysis

	(1)	(2)	(3)	(4)
VARIABLES	S&A$_{sales}$	S&A$_{sales}$	S&A$_{sales}$	S&A$_{sales}$
Security Score	0.000748	0.000881*	0.000770	0.000632
	(0.000584)	(0.000495)	(0.000543)	(0.000754)
Cyber Insurance	0.00519	0.0142	0.00664	-0.00275
	(0.0210)	(0.0183)	(0.0196)	(0.0267)
Security Score × Cyber Insurance	0.000189	-0.000131	0.000137	0.000471
	(0.000902)	(0.000809)	(0.000846)	(0.00115)
Size	-0.0152***	-0.00956**	-0.0143***	-0.0202***
	(0.00440)	(0.00386)	(0.00413)	(0.00557)
Age	-0.0129*	-0.00631	-0.0118*	-0.0187**
	(0.00697)	(0.00662)	(0.00665)	(0.00828)
Tobin's Q	0.0226***	0.0204***	0.0222***	0.0245***
	(0.00362)	(0.00352)	(0.00347)	(0.00421)
Leverage	-0.0604*	-0.0383	-0.0568*	-0.0799**
	(0.0314)	(0.0286)	(0.0297)	(0.0382)
Profit Margin	-1.365***	-1.124***	-1.326***	-1.578***
	(0.265)	(0.206)	(0.245)	(0.352)
Sales Growth	-0.0427	-0.0397*	-0.0422*	-0.0453
	(0.0264)	(0.0210)	(0.0243)	(0.0354)
Capex	0.0778	0.0821	0.0785	0.0740
	(0.0692)	(0.0682)	(0.0661)	(0.0817)
Asset Tangibility	-0.0886***	-0.100***	-0.0905***	-0.0782**
	(0.0307)	(0.0284)	(0.0291)	(0.0370)
R&D	0.332***	0.271***	0.322***	0.385***
	(0.0422)	(0.0470)	(0.0416)	(0.0430)
Constant	0.366***	0.224***	0.343***	0.492***
	(0.0460)	(0.0398)	(0.0435)	(0.0588)
Observations	1,306	1,306	1,306	1,306
R-squared	0.584			
Regression Type	OLS	Quantile	Quantile	Quantile
Quantileth	None	25	50	75
Industry fixed effects	Yes	Yes	Yes	Yes
Year-Quarter fixed effects	Yes	Yes	Yes	Yes

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Table 4: This table presents regressions on R&D$_{sales}$, defined as R&D to Sales, for firms that have yet to experience a data breach and are subjected to potential future breaches. The primary variable of interest is the securityscorecard, the transformed variable from the securityscorecard score as detailed in the data sections. The control and primary variables are all lagged by one period, including Size, Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capex, Asset Tangibility, R&D, and Probability of Breach. Firm Age is defined as the natural logarithm of the firm's Age, and Firm Size is defined as the natural logarithm of total assets. Sales Growth is defined as the change in sales from the previous period: $(sale_t/(sale_{t-1} - 1))$, Profit Margin is defined as EBITDA over total assets: $ebitda/at$, Capital Expenditures is defined as capital expenditure over property, plant, and equipment: $capx/ppent$, Tobin's Q is defined as adjusted assets over total assets: $(at - ceq + (prcc_f \times csho))/at$, Leverage is defined as long-term debt over total assets: $dltt/at$, Asset Tangibility is defined as the ratio of tangible assets to total assets, and R&D Expenditures is defined as R&D over total assets: xrd/at. The significance levels are denoted by * for $p < 0.1$, ** for $p < 0.05$, and *** for $p < 0.01$

regressions analysis

	(1)	(2)	(3)	(4)
VARIABLES	R&D$_{sales}$	R&D$_{sales}$	R&D$_{sales}$	R&D$_{sales}$
Security Score	0.000218	0.000288*	0.000244	0.000156
	(0.000235)	(0.000159)	(0.000192)	(0.000338)
Cyber Insurance	0.00153	0.00157	0.00154	0.00149
	(0.00937)	(0.00652)	(0.00764)	(0.0137)
Security Score × Cyber Insurance	0.000133	3.29e-05	9.62e-05	0.000222
	(0.000422)	(0.000289)	(0.000339)	(0.000633)
Size	0.00533***	0.00380***	0.00476***	0.00668***
	(0.00184)	(0.00134)	(0.00155)	(0.00257)
Age	-0.00378	0.000873	-0.00205	-0.00785*
	(0.00321)	(0.00237)	(0.00272)	(0.00443)
Tobin's Q	0.00635***	0.00442***	0.00564***	0.00805***
	(0.00160)	(0.00133)	(0.00141)	(0.00212)
Leverage	-0.0451***	-0.0213**	-0.0363***	-0.0661***
	(0.0123)	(0.00927)	(0.0106)	(0.0166)
Profit Margin	-0.383***	-0.245**	-0.332***	-0.505***
	(0.119)	(0.107)	(0.109)	(0.147)
Sales Growth	-0.0345***	-0.0289***	-0.0325***	-0.0395**
	(0.0124)	(0.00900)	(0.0105)	(0.0167)
Capex	0.0355	0.0215	0.0303	0.0477
	(0.0345)	(0.0260)	(0.0294)	(0.0471)
Asset Tangibility	0.00762	0.00401	0.00628	0.0108
	(0.0110)	(0.00667)	(0.00881)	(0.0159)
R&D	0.254***	0.193***	0.231***	0.307***
	(0.0273)	(0.0282)	(0.0270)	(0.0287)
Constant	-0.0120	-0.0380***	-0.0216	0.0108
	(0.0214)	(0.0146)	(0.0177)	(0.0302)
Observations	1,306	1,306	1,306	1,306
R-squared	0.602			
Regression Type	OLS	Quantile	Quantile	Quantile
Quantileth	None	25	50	75
Industry fixed effects	Yes	Yes	Yes	Yes
Year-Quarter fixed effects	Yes	Yes	Yes	Yes

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Table 5: This table presents logistics regressions. The primary variables of interest are the securityscorecard, the transformed variable from the security scorecardscore as detailed in the data sections, and Cyber insurance. The control and primary variables are all lagged by three quarters, including Size, Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capex, Asset Tangibility, R&D, and Probability of Breach. Firm Age is defined as the natural logarithm of the firm's Age, and Firm Size is defined as the natural logarithm of total assets. Sales Growth is defined as the change in sales from the previous period: $(sale_t/(sale_{t-1} - 1))$, Profit Margin is defined as EBITDA over total assets: $ebitda/at$, Capital Expenditures is defined as capital expenditure over property, plant, and equipment: $capx/ppent$, Tobin's Q is defined as adjusted assets over total assets: $(at - ceq + (prcc_f \times csho))/at$, Leverage is defined as long-term debt over total assets: $dltt/at$, Asset Tangibility is defined as the ratio of tangible assets to total assets, and R&D Expenditures is defined as R&D over total assets: xrd/at. The significance levels are denoted by * for p < 0.1, ** for p < 0.05, and *** for p < 0.01

Logit Regression Analysis

VARIABLES	Breach
Security Score	-0.000464
	(0.0198)
Cyber Insurance	0.961**
	(0.474)
Size	0.784***
	(0.212)
Age	-0.465
	(0.404)
Tobin's Q	0.0841
	(0.230)
Leverage	3.179***
	(1.128)
Profit Margin	0.213
	(10.49)
Sales Growth	-0.378
	(0.681)
Capex	-1.685
	(3.522)
Asset Tangibility	-0.814
	(1.337)
R&D	2.043
	(1.725)
Observations	547
Industry Fixed Effects	Yes
Year-Quarter Fixed Effects	Yes
Cluster Std Error	Firm

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Table 6: This table provides insights into the relationship between the unexpected Scope of a data breach (positive and negative deviations from the mean) and the cumulative abnormal returns (CARs) during various event windows surrounding the breach conditioning on Cyber Insurance. The regressions are presented for three distinct temporal spans. Key independent variables, Unexpected Scope mean $_{\text{mean}}$ $(+)$ and Unexpected Scope mean $_{\text{mean}}$ $(-)$, represent positive and negative deviations from the mean Scope of prior breaches, respectively. The Unexpected $Scope_{\text{mean}}$ quantifies the difference between the current Scope and the average Scope from prior breaches since the start of the sample period. Unexpected Scope $_{(\text{mean}}$ $(+)$ measures the positive deviation of the current Scope from previous breaches' average Scope within the sample duration, or zero otherwise. Conversely, Unexpected Scope $_{\text{mean}}$ $(-)$ calculates any negative deviation, defaulting to zero if there isn't one. Control variables are also included: Size accounts for the firm's magnitude, Profit Margin captures profitability, and Leverage indicates the proportion of borrowed capital used in the firm's operations. Standard errors, encapsulated in parentheses below each coefficient, denote the accuracy of the estimates. The significance levels are highlighted using asterisks: $***$ indicating p-value less than 0.01, ** signifying p-value less than 0.05 , and $*$ denoting p-value less than 0.1 . Year- and industry-specific fixed effects have been incorporated to exclude external time and industry variations. Additionally, robust clustered standard errors address potential data clustering issues.

	CAR$(-1,+1)$	CAR$(-3,+3)$	CAR$(-5,+5)$
VARIABLES	(2)	(4)	(6)
Unexpected Scope $(-)$	-0.00254	-0.00630	-0.0100
	(0.00335)	(0.00432)	(0.00614)
Unexpected Scope $(+)$	-0.000343***	-0.000383***	-0.000262
	(6.01e-05)	(9.07e-05)	(0.000170)
Cyber Insurance	0.00300	-0.000988	0.00204
	(0.00549)	(0.00975)	(0.0140)
Unexpected Scope $(-)$ × Cyber Insurance	0.00399	0.00477	0.00610
	(0.00555)	(0.00827)	(0.0110)
Unexpected Scope $(+)$ × Cyber Insurance	-0.00135***	-0.00132***	-0.000401
	(0.000178)	(0.000355)	(0.000483)
Size	0.00248**	0.00269	0.00397*
	(0.00116)	(0.00181)	(0.00223)
Return on Asset	0.0131	0.0110	0.00588
	(0.0149)	(0.0262)	(0.0396)
Leverage	-0.0337**	-0.0470**	-0.0773***
	(0.0154)	(0.0195)	(0.0286)
Constant	-0.0285***	-0.0279	-0.0349
	(0.0102)	(0.0171)	(0.0223)
Observations	344	344	344
R-squared	0.225	0.223	0.212
Year Fixed Effects	Yes	Yes	Yes
Industry Fixed Effects	Yes	Yes	Yes
Firm Cluster Std. Error	Yes	Yes	Yes

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

8 References

Abbiati, Giovanni, Silvio Ranise, Antonio Schizzerotto, and Alberto Siena. 2021. "Merging Datasets of CyberSecurity Incidents for Fun and Insight." *Frontiers in Big Data* 3 (January): 521132. https://doi.org/10.3389/fdata.2020.521132.

Akey, Pat, Stefan Lewellen, and Inessa Liskovich. 2018. "Hacking Corporate Reputations." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3143740.

Alex Blau. 2019. *Cybersecurity: Insights You Need from Harvard Business Review*. Insights You Need from Harvard Business Review. Boston, Massachusetts: Harvard Business Review Press.

alliance, cyber management. 2023. "Why Do Cyber Insurance Claims Get Rejected?" https://www.cm-alliance.com/cybersecurity-blog/why-do-cyber-insurance-claims-get-rejected#.

Andrea Vittorio. 2022. "Merck's $1.4 Billion Insurance Win Splits Cyber From 'Act of War'." https://news.bloomberglaw.com/privacy-and-data-security/mercks-1-4-billion-insurance-win-splits-cyber-from-act-of-war.

Aziz, Baharuddin, Suhardi, and Kurnia. 2020. "2020 International Conference on Information Technology Systems and Innovation (ICITSI)." In, 357–63. Bandung - Padang, Indonesia: IEEE. https://doi.org/10.1109/ICITSI50517.2020.9264966.

Bailey, Liam M D. 2014. "Mitigating Moral Hazard in Cyber-Risk Insurance." *Journal of Law & Cyber Warfare* 3.

Boasiako, Kwabena Antwi, and Michael O'Connor Keefe. 2021. "Data Breaches and Firm Credit Risk." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3782111.

Bob Zukis. 2021. "How Cyber Insurance Actually Increased Cyber Risk." https://www.forbes.com/sites/bobzukis/2021/03/25/has-cyber-insurance-actually-increased-cyber-risk/?sh=cf5fa7b46d8d.

Coble, Sarah. 2021. "American Companies Not Taking Cybersecurity Seriously." https://www.infosecurity-magazine.com/news/us-companies-lynx-survey/.

Cohn, Carolyn. 2021. "Focus: Insurers Run from Ransomware Cover as Losses Mount." *Reuters*, November. https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/.

Crosignani, Matteo, Marco Macchiavelli, and Andre F Silva. 2021. "Pirates Without Borders: The Propagation of Cyberattacks Through Firms' Supply Chains." *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2022.12.002.

Eling, Martin, Michael McShane, and Trung Nguyen. 2021. "Cyber Risk Management: History and Future Research Directions." *Risk Management and Insurance Review* 24 (1): 93–125. https://doi.org/10.1111/rmir.12169.

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber. 2022. "Cybersecurity Risk." Edited by Itay Goldstein. *The Review of Financial Studies* 36 (1): 351–407. https://doi.org/10.1093/rfs/hhac024.

Francis, Bill B., Wenyao Hu, and Thomas D. Shohfi. 2021. "Ex-Intrusion Corporate Cyber Risk: Evidence from Internet Protocol Networks." *Journal of Operational Risk*, September. https://www.risk.net/node/7879801.

Garcia, Ahiza. 2015. "Target Settles for $39 Million over Data Breach." https://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/index.html.

Gatzlaff, and McCullough. 2010. "The Effect of Data Breaches on Shareholder Wealth." https://doi.org/10.1111/j.1540-6296.2010.01178.x.

Goode, Sigi, Hartmut Hoehle, Viswanath Venkatesh, and Susan A. Brown. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach." *MIS Quarterly* 41 (3): 703–A16. https://www.jstor.org/stable/26635011.

Gwebu, Kholekile L., Jing Wang, and Li Wang. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management." *Journal of Management Information Systems* 35 (2): 683–714. https://doi.org/10.1080/07421222.2018.1451962.

Han, Seungjin, and Jiaping Qiu. 2007. "Corporate Precautionary Cash Holdings." *Journal of Corporate Finance* 13 (1): 43–57. https://doi.org/10.1016/j.jcorpfin.2006.05.002.

Hsu, Po-Hsuan, Wei-Chuan Kao, and Yanzhi Wang. 2021. "Cybersecurity and Brand Capital," December.

Jamilov, Rustam, Hélène Rey, and Ahmed Tahoun. 2021. "The Anatomy of Cyber Risk." w28906. Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w28906.

Janakiraman, Ramkumar, Joon Ho Lim, and Rishika Rishika. 2018. "The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer." *Journal of Marketing* 82 (2): 85–105. https://www.jstor.org/stable/44878206.

Jiang, Erica Xuewei, Gloria Yang Yu, and Jinyuan Zhang. 2022. "Bank Competition Amid Digital Disruption: Implications for Financial Inclusion." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4178420.

Jonathan Stempel. 2015. "Target in $39.4 Million Settlement with Banks over Data Breach." *Reuters*, December. https://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203.

Josephine Wolff. 2021. "How the NotPetya Attack Is Reshaping Cyber Insurance." https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M. Stulz. 2021. "Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms." *Journal of Financial Economics* 139 (3): 719–49. https://doi.org/10.1016/j.jfineco.2019.05.019.

Kevin Collier. 2023. "Top Cyber Official Offers 'Stark Warning' of Attacks by China on U.S. Infrastructure." https://www.nbcnews.com/tech/security/top-us-cyber-official-warns-infrastructure-attack-risk-china-tensions-rcna99625.

Khallaf, Ashraf. 2012. "Information Technology Investments and Nonfinancial Measures: A

Research Framework." *Accounting Forum* 36 (2): 109–21. https://doi.org/10.1016/j.accfor.2011.07.001.

Kieschnick, Robert, Wendy Rotenberg, and Kai-Sheng Song. 2023. "On the Conditional Analysis of Skewed Variables in Corporate Finance."

Lattanzio, Gabriele, and Yue Ma. 2023. "Cybersecurity Risk and Corporate Innovation." *Journal of Corporate Finance*, June, 102445. https://doi.org/10.1016/j.jcorpfin.2023.102445.

Lending, Claire, Kristina Minnick, and Patrick J. Schorno. 2018. "Corporate Governance, Social Responsibility, and Data Breaches." *Financial Review* 53 (2): 413–55. https://doi.org/10.1111/fire.12160.

Lim, Jee-Hae, Bruce Dehning, Vernon J. Richardson, and Rodney E. Smith. 2011. "A Meta-Analysis of the Effects of IT Investment on Firm Financial Performance." *Journal of Information Systems* 25 (2): 145–69. https://doi.org/10.2308/isys-10125.

Loughran, Tim, and Bill Mcdonald. 2011. "When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks." *The Journal of Finance* 66 (1): 35–65. https://doi.org/10.1111/j.1540-6261.2010.01625.x.

Majuca, Ruperto P, William Yurcik, and Jay P Kesan. 2006. "THE EVOLUTION OF CYBERINSURANCE."

Makridis, Christos A. 2021. "Do Data Breaches Damage Reputation? Evidence from 45 Companies Between 2002 and 2018." *Journal of Cybersecurity* 7 (1): tyab021. https://doi.org/10.1093/cybsec/tyab021.

Marotta, Angelica, Fabio Martinelli, Stefano Nanni, Albina Orlando, and Artsiom Yautsiukhin. 2017. "Cyber-Insurance Survey." *Computer Science Review* 24 (May): 35–61. https://doi.org/10.1016/j.cosrev.2017.01.001.

Michael Kassner. 2015. "Data Breaches May Cost Less Than the Security to Prevent Them." https://www.yahoo.com/tech/s/data-breaches-may-cost-less-194542581.html.

Miller, Lauren. 2019. "Cyber Insurance: An Incentive Alignment Solution to Corporate Cyber-Insecurity." *Journal of Law & Cyber Warfare* 7.

NAIC Staff. 2022. "Report on the Cyber Insurance Market." https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf.

Nancy Gohring. 2002. "Cyberinsurance May Cover Damage of Computer Woes." *Seattle Times*. https://www.seattletimes.com/.

Network, European, and Information Security Agency. 2012. "Incentives and Barriers of the Cyber Insurance Market in Europe."

Orr, Susan. 2021. "Cyberattacks Prompt Higher Insurance Premiums, Lower Coverage Limits."

Oyima-Antseleve, Ndackyssa. 2023. "Expectations, Data Breaches, and Shareholder Wealth."

Ponemon Institute LLC. 2013. "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age."

Protection, National, and Programs Directorate U. S. Department of Homeland Security. 2012. “Cybersecurity Insurance Workshop.” https://www.cisa.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf.

PWC. 2016. “The Promise and Pitfalls of Cyber Insurance.” https://www.pwc.com/us/en/insurance/publications/assets/pwc-insurance-top-issues-cyber-insurance.pdf.

Romanosky, Sasha, Lillian Ablon, Andreas Kuehn, and Therese Jones. 2019. “Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?” *Journal of Cybersecurity* 5 (1). https://doi.org/10.1093/cybsec/tyz002.

SEC. 2011. “CF Disclosure Guidance: Topic No. 2 - Cybersecurity.” October 13, 2011. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

———. 2018. “Commission Statement and Guidance on Public Company Cybersecurity Disclosures,” February.

———. 2022. “SEC.gov | SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies.” 2022. https://www.sec.gov/news/press-release/2022-39.

———. 2023. “SEC.gov | Cybersecurity.” 2023. https://www.sec.gov/news/press-release/2023-52.

Sheridan, Kelly. 2020. “Missing Patches, Misconfiguration Top Technical Breach Causes.” https://www.darkreading.com/vulnerabilities-threats/missing-patches-misconfiguration-top-technical-breach-causes.

Shevchenko, Pavel V, Jiwook Jang, Matteo Malavasi, Gareth W Peters, Georgy Sofronov, and Stefan Trück. 2023. “The Nature of Losses from Cyber-Related Events: Risk Categories and Business Sectors.” *Journal of Cybersecurity* 9 (1): tyac016. https://doi.org/10.1093/cybsec/tyac016.

Smith, Zhanna Malekos, Eugenia Lostri, and James A Lewis. 2020. “The Hidden Costs of Cybercrime.” https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf.

Sohval, Bob. 2023. “A Deep Dive in Scoring Methodology.”

Swiss Re Institute. 2022. “Cyber Insurance: Strengthening Resilience for the Digital Transformation.” https://www.swissre.com/dam/jcr:6fd9f6dd-4631-4d9f-9c3b-5a3b79b321c0/2022-11-08-sri-expertise-publication-cyber-insurance-strengthening-resilience.pdf.

Verizon. 2022. “2022-Data-Breach-Investigations-Report-Dbir.pdf.” https://www.verizon.com/business/resources/Tc5c/reports/dbir/2022-data-breach-investigations-report-dbir.pdf.

Zafar, Humayun, Myung S. Ko, and Kweku-Muata Osei-Bryson. 2016. “The Value of the CIO in the Top Management Team on Performance in the Case of Information Security Breaches.” *Information Systems Frontiers* 18 (6): 1205–15. https://doi.org/10.1007/s10796-015-9562-5.

9 Appendix

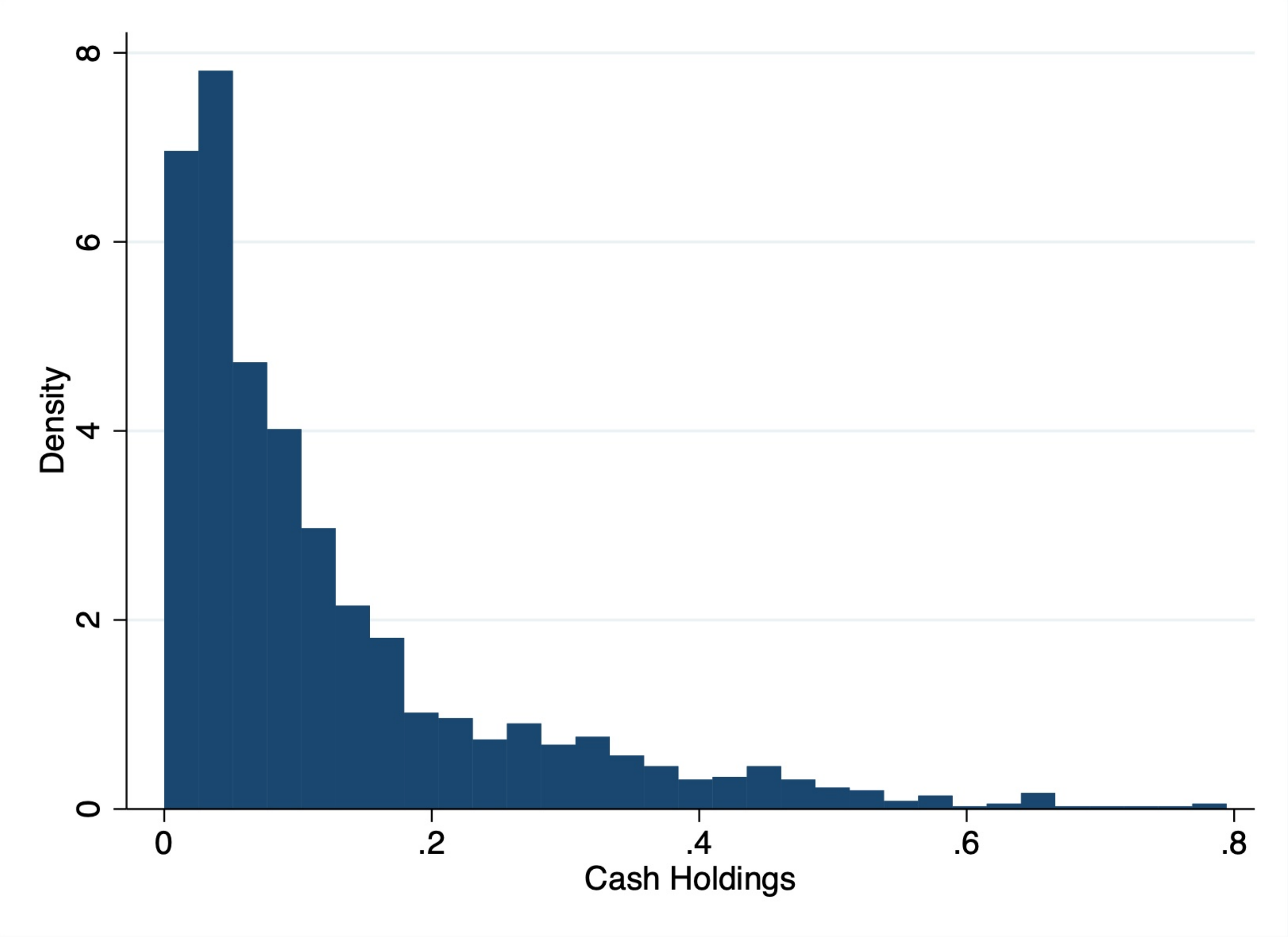


Figure 2: This graphic showcases the histograms for cash holdings

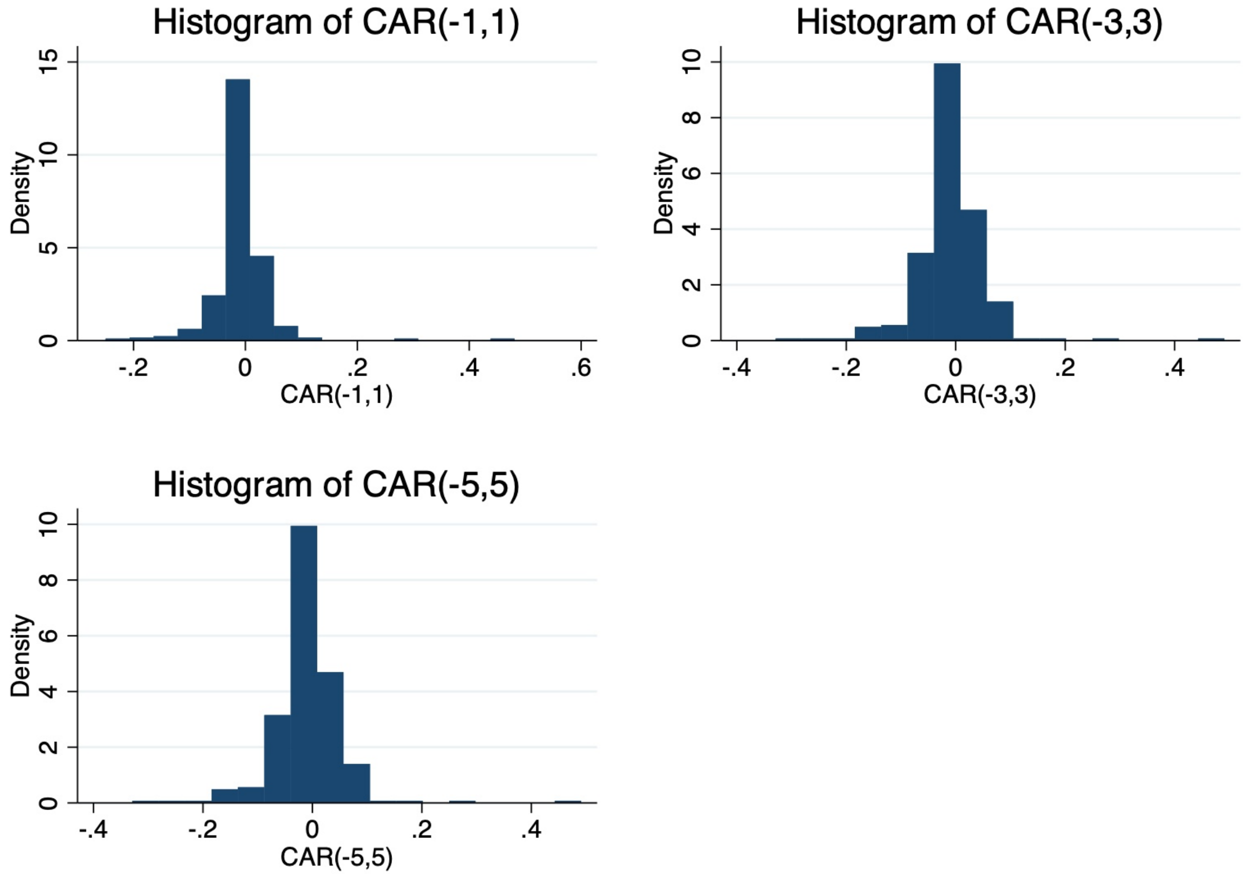


Figure 3: This graphic showcases the histograms for each of the specified variables: CAR(-1,1), CAR(-3,3), CAR(-5,5)

Table 7: This table provides summary statistics of the variables used in subsequent analysis. The indicator variable representing cyber insurance in a firm's 10-K documents is nuanced. It is assigned a value of 1 when terms related to cyber insurance are mentioned, determined by the presence of National Initiative for Cybersecurity Careers and Studies (NICCS) keywords within ten words before or after the word "insurance" in the 10-K documents. Additionally, the variable takes the value of 1 when firms explicitly state in their 10-Ks that they have cyber insurance. The ex-ante probability of a breach (Probability Breach) is estimated using the prior breach history of firms, utilizing data from the beginning of the sample period up to the year preceding the actual estimation year. Cyber Score Oyima is a weighted word count constructed where weights were calculated using the methodology of Loughran and McDonald (2011), following Lattanzio et al. (2023) to develop a 10-K disclosures-based measure with a comprehensive dictionary. Cyber Score Florackis et al. (2022) is based on the 10-K cybersecurity risk measure provided by Florackis et al. (2022). The other variables being assessed in this context include Size, Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capex, Asset Tangibility, R&D, and Probability of Breach : Firm Age (defined as the log of the firm's age), Firm Size (defined as the log of total assets), Sales Growth (defined as the change in sales from the previous period: $(sale_t/(sale_{t-1}-1)))$, Profit Margin (defined as EBITDA over total assets: $ebitda/at$), Capital Expenditures (defined as capital expenditure over property, plant, and equipment: $capx/ppent$), Tobin's Q (defined as adjusted assets over total assets: $(at - ceq + (prcc_f \times csho))/(at))$, Leverage (defined as long term debt over total assets: $dltt/at$), Asset Tangibility (defined as the ratio of tangible assets to total assets), R&D Expenditures (defined as R&D over total assets: xrd/at). The dependent variables - Receivables, Inventory, Payables, Notes Payables, Repurchases, and Cash Holdings ratios - are computed by dividing the respective balance sheet or income statement item of the next period (lagged one period) by the total assets of the current period.

	mean	sd	min	max
Cash	0.199	0.201	0.000	0.924
Receivables	0.136	0.109	0.000	0.593
Inventory	0.107	0.138	0.000	0.747
Payables	0.079	0.081	0.002	0.489
Note Payables	0.012	0.043	0.000	0.372
Probability Breach	0.025	0.050	0.000	0.417
Cyber Score Florackis et al.(2022)	0.367	0.185	0.000	0.652
Cyber Score Oyima (2023)	1.418	1.952	0.000	11.996
Cyber Insurance	0.110	0.312	0.000	1.000
Size	6.835	2.003	1.729	11.867
Age	3.025	0.635	1.386	4.234
Tobin's Q	2.098	1.436	0.486	10.103
Leverage	0.195	0.198	0.000	0.872
Profit Margin	0.075	0.184	-1.151	0.447
Sales Growth	0.094	0.362	-0.828	4.604
Capex	0.044	0.046	0.000	0.314
Asset Tangibility	0.220	0.218	0.002	0.926
R&D	0.052	0.099	0.000	0.677
Observations	12524			

Table 8: This table provides a correlation matrix showcasing the relationship between various measures of company performance and risk. The variables include Probability of Breach, Cyber Risk Score from Florackis et al 2022, and the Cyber Risk Score I constructed, Company Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capital Expenditure (Capex), Asset Tangibility, R&D Expenditure, Cash Holdings, Receivables, Inventory, Payables, Notes Payables, and Short-Term Debt. The correlation coefficients range between -1 and 1, indicating the strength and direction of the relationship between the pairs of variables. P-values are reported below the coefficients in parentheses, indicating the statistical significance of the correlations.

Variables	Probability Breach	Cyber Score Fl.	Cyber Score O.	Cyber Insurance	Cash	Receivables	Inventory	Payables	Note Payables	Short-Term Debt	Repurchases	Dividents Payout	Long-Term Debt	Size	Age	Tobin's Q	Leverage	Profit Margin	Sales Growth	Capex	Asset Tangibility	R &D
Probability Breach	1.000																					
Cyber Score Fl.	0.133	1.000																				
	(0.000)																					
Cyber Score O.	0.101	0.214	1.000																			
	(0.000)	(0.000)																				
Cyber Insurance	0.060	0.089	0.445	1.000																		
	(0.000)	(0.000)	(0.000)																			
Cash	-0.118	0.032	0.109	0.074	1.000																	
	(0.000)	(0.001)	(0.000)	(0.000)																		
Receivables	-0.080	-0.060	0.001	0.024	-0.048	1.000																
	(0.000)	(0.000)	(0.924)	(0.011)	(0.000)																	
Inventory	0.000	-0.017	-0.133	-0.047	-0.188	0.013	1.000															
	(0.997)	(0.059)	(0.000)	(0.000)	(0.000)	(0.164)																
Payables	0.055	-0.014	-0.044	0.004	-0.104	0.398	0.436	1.000														
	(0.000)	(0.122)	(0.000)	(0.664)	(0.000)	(0.000)	(0.000)															
Note Payables	-0.006	-0.059	-0.040	-0.016	-0.074	0.133	0.186	0.105	1.000													
	(0.487)	(0.000)	(0.000)	(0.087)	(0.000)	(0.000)	(0.000)	(0.000)														
Short-Term Debt	0.006	-0.057	-0.044	-0.020	-0.071	0.106	0.123	0.076	0.709	1.000												
	(0.533)	(0.000)	(0.000)	(0.029)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)													
Repurchases	0.178	0.079	0.100	0.052	0.015	-0.054	-0.030	-0.045	-0.024	-0.043	1.000											
	(0.000)	(0.000)	(0.000)	(0.000)	(0.102)	(0.000)	(0.001)	(0.000)	(0.009)	(0.000)												
Dividents Payout	0.099	0.040	-0.015	0.001	-0.068	-0.025	-0.002	-0.010	-0.008	-0.034	0.025	1.000										
	(0.000)	(0.000)	(0.099)	(0.898)	(0.000)	(0.008)	(0.821)	(0.280)	(0.395)	(0.000)	(0.006)											
Long-Term Debt	0.113	0.081	-0.024	-0.027	-0.201	-0.088	-0.051	-0.058	-0.060	0.008	0.001	0.060	1.000									
	(0.000)	(0.000)	(0.009)	(0.003)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.405)	(0.878)	(0.000)										
Size	0.540	0.128	0.053	0.004	-0.323	-0.152	-0.024	-0.026	-0.040	-0.049	0.170	0.134	0.298	1.000								
	(0.000)	(0.000)	(0.000)	(0.643)	(0.000)	(0.000)	(0.009)	(0.004)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)									
Age	0.279	0.048	-0.073	-0.028	-0.262	0.032	0.141	0.069	0.018	-0.016	0.052	0.113	0.033	0.377	1.000							
	(0.000)	(0.000)	(0.000)	(0.002)	(0.000)	(0.001)	(0.000)	(0.000)	(0.057)	(0.079)	(0.000)	(0.000)	(0.000)	(0.000)								
Tobin's Q	-0.001	0.118	0.090	0.061	0.419	-0.013	-0.128	-0.064	-0.034	-0.026	0.196	0.026	-0.020	-0.133	-0.181	1.000						
	(0.952)	(0.000)	(0.000)	(0.000)	(0.000)	(0.167)	(0.000)	(0.000)	(0.000)	(0.005)	(0.000)	(0.004)	(0.027)	(0.000)	(0.000)							
Leverage	0.128	0.058	-0.034	-0.030	-0.308	-0.186	-0.079	-0.110	-0.052	0.099	-0.042	0.049	0.800	0.341	0.058	-0.097	1.000					
	(0.000)	(0.000)	(0.000)	(0.001)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)						
Profit Margin	0.177	0.033	-0.004	-0.001	-0.343	0.071	0.092	-0.010	-0.050	-0.101	0.269	0.141	0.092	0.415	0.233	-0.076	0.090	1.000				
	(0.000)	(0.000)	(0.656)	(0.909)	(0.000)	(0.000)	(0.000)	(0.302)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)					
Sales Growth	-0.036	0.018	-0.000	0.006	0.160	-0.001	-0.049	-0.034	-0.019	-0.009	-0.016	-0.046	0.047	-0.039	-0.151	0.230	-0.014	-0.058	1.000			
	(0.000)	(0.055)	(0.997)	(0.499)	(0.000)	(0.941)	(0.000)	(0.000)	(0.041)	(0.352)	(0.089)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.118)	(0.000)				
Capex	-0.042	-0.002	-0.079	-0.052	-0.154	-0.194	-0.057	0.001	-0.049	-0.013	-0.004	0.001	0.102	0.079	-0.026	0.028	0.106	0.143	-0.002	1.000		
	(0.000)	(0.820)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.917)	(0.000)	(0.153)	(0.701)	(0.934)	(0.000)	(0.000)	(0.004)	(0.002)	(0.000)	(0.000)	(0.798)			
Asset Tangibility	-0.004	-0.052	-0.152	-0.096	-0.322	-0.310	-0.065	-0.046	-0.042	0.008	-0.053	0.058	0.232	0.205	0.098	-0.172	0.293	0.149	-0.080	0.682	1.000	
	(0.697)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.394)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)		
R &D	-0.132	-0.011	0.081	0.059	0.555	-0.033	-0.159	-0.094	-0.039	-0.015	-0.058	-0.101	-0.155	-0.359	-0.208	0.327	-0.196	-0.596	0.112	-0.161	-0.293	1.00 > 0
	(0.000)	(0.232)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.107)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0. > 000)	

Table 9: This table presents regressions for firms that have not yet experienced a data breach and are subjected to potential future breaches. The primary variable of interest is the Cyber Risk Score **(Cyber Score O.)**, based on 10-K disclosure; the higher the score, the higher the risk. The control and primary variables are all lagged by one period, including Size, Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capex, Asset Tangibility, R&D, and Probability of Breach. Firm Age is defined as the natural logarithm of the firm's Age, and Firm Size is defined as the natural logarithm of total assets. Sales Growth is defined as the change in sales from the previous period: $(sale_t/(sale_{t-1} - 1))$, Profit Margin is defined as EBITDA over total assets: $ebitda/at$, Capital Expenditures is defined as capital expenditure over property, plant, and equipment: $capx/ppent$, Tobin's Q is defined as adjusted assets over total assets: $(at - ceq + (prcc_f \times csho))/at$, Leverage is defined as long-term debt over total assets: $dltt/at$, Asset Tangibility is defined as the ratio of tangible assets to total assets, and R&D Expenditures is defined as R&D over total assets: xrd/at. The significance levels are denoted by * for $p < 0.1$, ** for $p < 0.05$, and *** for $p < 0.01$

regressions analysis

	(1)	(2)	(3)	(4)
VARIABLES	Cash	Cash	Cash	Cash
Cyber Score O.	0.000240	-0.000948	-5.13e-05	0.00123
	(0.00194)	(0.00155)	(0.00179)	(0.00254)
Cyber Insurance	-0.0216	-0.0312***	-0.0240*	-0.0136
	(0.0140)	(0.0119)	(0.0131)	(0.0180)
Cyber Score O. × Cyber Insurance	0.00792**	0.00988***	0.00840***	0.00628
	(0.00319)	(0.00265)	(0.00296)	(0.00419)
Size	-0.00542***	0.00460***	-0.00296	-0.0138***
	(0.00195)	(0.00164)	(0.00183)	(0.00252)
Age	-0.0224***	-0.0202***	-0.0218***	-0.0241***
	(0.00450)	(0.00415)	(0.00429)	(0.00556)
Tobin's Q	0.0244***	0.0183***	0.0229***	0.0295***
	(0.00262)	(0.00272)	(0.00258)	(0.00295)
Leverage	-0.192***	-0.170***	-0.187***	-0.211***
	(0.0147)	(0.0105)	(0.0131)	(0.0209)
Profit Margin	-0.111***	-0.0778***	-0.103***	-0.140***
	(0.0227)	(0.0216)	(0.0219)	(0.0270)
Sales Growth	-0.00391	-0.00693	-0.00465	-0.00139
	(0.00609)	(0.00501)	(0.00562)	(0.00815)
Capex	-0.0765	-0.0206	-0.0628	-0.123*
	(0.0517)	(0.0459)	(0.0488)	(0.0660)
Asset Tangibility	-0.135***	-0.0593***	-0.116***	-0.197***
	(0.0174)	(0.0140)	(0.0160)	(0.0236)
R&D	0.612***	0.611***	0.612***	0.613***
	(0.0485)	(0.0524)	(0.0484)	(0.0526)
Constant	0.298***	0.117***	0.253***	0.449***
	(0.0193)	(0.0184)	(0.0191)	(0.0246)
Observations	10,736	10,736	10,736	10,736
R-squared	0.506			
Regression Type	OLS	Quantile	Quantile	Quantile
Quantileth	None	25	50	75
Industry fixed effects	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes

Robust standard clustered errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

Table 10: This table presents regressions for firms that have not yet experienced a data breach and are subjected to potential future breaches. The primary variable of interest is the ex-ante breach probability, using a logistic regression based on prior breach history. The control and primary variables are all lagged by one period, including Size, Age, Tobin's Q, Leverage, Profit Margin, Sales Growth, Capex, Asset Tangibility, R&D, and Probability of Breach. Firm Age is defined as the natural logarithm of the firm's Age, and Firm Size is defined as the natural logarithm of total assets. Sales Growth is defined as the change in sales from the previous period: $(sale_t/(sale_{t-1}-1))$, Profit Margin is defined as EBITDA over total assets: $ebitda/at$, Capital Expenditures is defined as capital expenditure over property, plant, and equipment: $capx/ppent$, Tobin's Q is defined as adjusted assets over total assets: $(at - ceq + (prcc_f \times csho))/at$, Leverage is defined as long-term debt over total assets: $dltt/at$, Asset Tangibility is defined as the ratio of tangible assets to total assets, and R&D Expenditures is defined as R&D over total assets: xrd/at. The significance levels are denoted by * for $p < 0.1$, ** for $p < 0.05$, and *** for $p < 0.01$

regressions analysis

	(1)	(2)	(3)	(4)
VARIABLES	Cash	Cash	Cash	Cash
Probability Breach	-0.146	-0.170	-0.152	-0.127
	(0.161)	(0.124)	(0.147)	(0.219)
Cyber Insurance	-0.0164	-0.0291*	-0.0194	-0.00579
	(0.0217)	(0.0168)	(0.0198)	(0.0297)
Probability Breach × Cyber Insurance	0.806	0.845*	0.815	0.774
	(0.610)	(0.449)	(0.559)	(0.808)
Size	-0.00441*	0.00557***	-0.00204	-0.0127***
	(0.00231)	(0.00199)	(0.00219)	(0.00297)
Age	-0.0224***	-0.0197***	-0.0218***	-0.0247***
	(0.00453)	(0.00416)	(0.00432)	(0.00563)
Tobin's Q	0.0247***	0.0186***	0.0232***	0.0298***
	(0.00262)	(0.00274)	(0.00259)	(0.00293)
Leverage	-0.195***	-0.173***	-0.189***	-0.213***
	(0.0147)	(0.0105)	(0.0132)	(0.0209)
Profit Margin	-0.113***	-0.0796***	-0.105***	-0.140***
	(0.0228)	(0.0216)	(0.0220)	(0.0272)
Sales Growth	-0.00413	-0.00733	-0.00489	-0.00147
	(0.00611)	(0.00502)	(0.00565)	(0.00816)
Capex	-0.0813	-0.0233	-0.0675	-0.129**
	(0.0516)	(0.0458)	(0.0487)	(0.0659)
Asset Tangibility	-0.137***	-0.0612***	-0.119***	-0.200***
	(0.0174)	(0.0139)	(0.0161)	(0.0238)
R&D	0.616***	0.614***	0.615***	0.618***
	(0.0487)	(0.0529)	(0.0486)	(0.0524)
Constant	0.295***	0.111***	0.251***	0.448***
	(0.0207)	(0.0193)	(0.0203)	(0.0265)
Observations	10,736	10,736	10,736	10,736
R-squared	0.504			
Regression Type	OLS	Quantile	Quantile	Quantile
Quantileth	None	25	50	75
Industry fixed effects	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes

Robust clustered standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1