Do Financial Markets Understand Cybersecurity: Evidence from a Direct Measure of Firm Network Vulnerabilities

Tim Liu and Christos A. Makridis*

July 22, 2026

Abstract

Despite the growing importance of cybersecurity, measuring cybersecurity exposures has proven challenging. Existing methods rely on textual and statistical analysis of disclosures, which require managers to have accurate appraisals of cybersecurity risks and disclose these risks in an unbiased manner. We introduce a novel firm-level measure of cybersecurity exposures that identify network ports accessible from the public internet, sidestepping the need to rely on managerial reporting. Our process replicates "port scans," a technique cybersecurity adversaries implement to identify vulnerable firms. We find that cybersecurity exposures predict future realized breaches. High cybersecurity exposure stocks underperform other stocks by 0.33% per month. Our findings differ from studies relying on disclosure-based measures of cybersecurity exposures, which find cybersecurity risk to be priced (higher exposures predicting higher returns). Our findings identify network exposures as an economically meaningful signal of the information security control environment and highlight limitations of disclosure-based assessments of cybersecurity risk.

*Tim Liu: University of Utah tim.liu@eccles.utah.edu. Christos Makridis: Arizona State University and Stanford University, cmakridi@stanford.edu. These views are our own and do not reflect those of any affiliated institutions. We thank Rapid7 for their academic partnership, especially Raj Samani, Deral Heiland, and Cynthia Wyre, as well as our academic partners, Kumar Shashwat and Dr. Xinming Ou at University of South Florida, for the extension of the data. Finally, we thank Erick Galinkin for his contributions to the project during his tenure at Rapid7.

1 Introduction

A foundational concern in accounting research is whether managers' disclosures and internal control systems give investors a faithful representation of the underlying risks that firms face (Jensen and Meckling, 1976; Leuz and Wysocki, 2016). Cybersecurity is a setting in which this concern is particularly acute. In particular, cybersecurity threats have consistently ranked among the top risks for doing business in North America (PwC, 2017; WEF, 2017), and the number of reported data breaches has risen by roughly 430% between 2005 and 2018 (CEA, 2019). Yet Amir et al. (2018) document that managers selectively withhold information about cyber incidents from investors, and the recent high-profile breaches of CDK Global and AT&T in 2024 suggest that the gap between firms' actual cybersecurity posture and what investors observe has not closed.[1] Existing measures of cybersecurity risk rely on managerial assessments embedded in financial statements and earnings calls (Florackis et al., 2023; Jamilov et al., 2023; Jiang et al., 2024; Sheneman, 2025). Textual risk disclosures are an imperfect proxy for underlying risk because they conflate the exposure itself with managerial attention to that exposure (Kravet and Muslu, 2013).

We examine whether a direct, externally replicable measure of firms' network-level cybersecurity exposures—constructed without reliance on managerial reporting—predicts realized breaches, future profitability, and equity returns. Our measure counts the number of high-risk network ports that are accessible from the public internet for each Fortune 500 firm in each month, replicating the "port scan" reconnaissance technique that adversaries use to identify exploitable systems. Because the measure is built from publicly observable network

[1] Source: Wall Street Journal, CDK and AT&T.

telemetry rather than from financial filings, it sidesteps two well-known sources of measurement error in this literature: (i) managerial discretion over what to disclose (Amir et al., 2018), and (ii) the conflation of true cybersecurity exposure with managerial concern about cybersecurity (Kravet and Muslu, 2013).

The setting is timely. Federal policy now requires continuous asset discovery on the premise that organizations themselves often lack reliable inventories of their internet-facing systems (Cybersecurity and Infrastructure Security Agency, 2022).[2] The setting also speaks to a long-standing accounting literature on internal controls and risk oversight. Ashbaugh-Skaife et al. (2009) and Doyle et al. (2007) document that weaknesses in internal control systems are associated with a higher cost of capital and poorer reporting quality, while Ashraf and Sunder (2023) provide evidence that mandated breach disclosure reduces shareholders' assessed cyber risk. Network-level exposures can be viewed as a control-environment signal specific to information security—one that is orthogonal to the narrative and accounting-based proxies that dominate the existing literature.

To construct the measure, we use Open Data from Rapid7, a cybersecurity advisory firm that operates an internet-scale telemetry platform (Galinkin et al., 2022). Rapid7 sends "probe packets" to each of the roughly 4.3 billion addresses in the IPv4 space; if a connection is established on a high-risk port, the address is flagged as exposed and, where possible, matched to a Fortune 500 firm.[3] Following Condon et al. (2023), we focus on four port categories that are widely recognized as exploitable when reachable from the public internet: Telnet (port 23, an unencrypted remote-login protocol), Server Message Block (SMB, ports

[2]Industry evidence corroborates this premise: exploitation of known, unpatched vulnerabilities remains a leading breach vector (Rapid7, 2020; Verizon, 2024).

[3]Since mapping IP addresses to firms is a time-intensive manual process, Rapid7 limits the scope of this matching exercise to Fortune 500 firms.

139 and 445, a file-sharing protocol), Secure Shell (SSH, port 22), and Remote Desktop Protocol (RDP, port 3389). The aggregate count of exposed high-risk ports across IP addresses affiliated with a firm in a given month is our measure of *Cybersecurity Exposures*. The measure is constructed from public information available to both adversaries and investors, bypassing the informational gatekeepers studied by Amir et al. (2018).

We begin by validating that *Cybersecurity Exposures* captures economically meaningful vulnerabilities. The median firm in our sample has five exposed high-risk ports. Firms with above-median exposures experience more than twice as many realized cybersecurity breaches over the sample period as firms with below-median exposures. While the measure is weakly correlated with the text-based risk score of Florackis et al. (2023), it is not statistically significant—consistent with our premise that disclosure-based and technical measures of cyber risk capture distinct constructs.

We argue that, if investors fully internalize cybersecurity exposures, high-exposure stocks should earn returns that compensate for bearing this risk; under-reaction or non-pricing, in contrast, would manifest as negative abnormal returns to exposed firms. We find evidence consistent with the second interpretation. A portfolio long high-exposure firms and short low-exposure firms generates a statistically significant equal-weighted excess return of -33 basis points per month (a value-weighted return of -78 basis points). For reference, Kamiya et al. (2021) document an equity value decline of 107 to 159 basis points in the week around *disclosed* breaches alone, and Dhaliwal et al. (2016) document a 21 basis point cost of equity effect for major customer concentration—placing our estimate in the same order of magnitude as comparable risk effects in the accounting literature. For the median Fortune 500 firm in our sample, the monthly differential translates to roughly $75 million in relative

market value. Fama–MacBeth regressions yield consistent inferences: high-exposure firms earn returns that are 29 to 42 basis points lower per month than low-exposure firms, after controlling for standard pricing factors.

We subject our finding to several sensitivity tests. Our inferences are robust to alternative expected return models (CAPM, Fama–French 3-Factor, Carhart 4-Factor, and Fama–French 5-Factor specifications), to a six-month rolling-average definition of exposures that mitigates concerns about monthly measurement noise, and to double sorts on size and book-to-market. In a horse race against the disclosure-based measure of Florackis et al. (2023), only our network-based measure retains predictive power for returns.

We next examine the mechanism. Three cross-sectional findings link exposures to future firm-level outcomes. First, a one standard deviation increase in *Cybersecurity Exposures* is associated with a 0.2 percentage point higher likelihood of an extreme negative (3σ) stock return in the following month—a meaningful increment relative to the unconditional probability of 0.8%. Second, a one standard deviation increase in exposures is associated with a 0.7 percentage point higher probability of a publicly disclosed breach in the following quarter, against an unconditional base rate of 1.4%. Third, average exposures over a quarter predict a 10-basis-point decline in next-quarter profitability, measured as EBITDA scaled by assets. Taken together, these results are consistent with network-level exposures translating into costly breach remediation that ultimately affects income.

We then ask why the equity market does not appear to price information that is, in principle, externally observable. We argue that reproducing the measure requires specialized knowledge of cybersecurity, networking, and programming that is uncommon among financial market participants; data from the American Community Survey indicate that fewer than

2% of workers in finance occupations hold a degree in computer or information sciences. Following Collins et al. (2003), we test whether the return effect concentrates in firms held disproportionately by less sophisticated investors. Consistent with an information-friction interpretation, negative abnormal returns to exposed firms are concentrated in firms with below-median investor sophistication, both in long–short portfolios and in Fama–MacBeth specifications interacting exposures with sophistication.

Finally, we investigate two frictions that may explain why firms allow exposures to persist. The first is a shortage of cybersecurity labor: industry estimates place the U.S. cybersecurity workforce gap at roughly 265,000 workers (Lightcast, 2024). We find that tightness in the local market for information security analysts is positively associated with exposures, the probability of an exposure manifesting as a realized breach, and the magnitude of negative returns to exposed firms. The second is managerial inattention. Consistent with Bana et al. (2022), firms that experienced a breach in the prior five years subsequently carry less than half the exposures of comparable firms and are nearly twice as likely to have an information security officer on the board, suggesting that breaches concentrate managerial attention onto cybersecurity issues. Negative returns to exposures are concentrated in firms without this attentional shock.

Notwithstanding the caveats we discuss in the conclusion, we contribute to the literature in three ways. First, we introduce a direct, externally replicable measure of firm-level cybersecurity exposure that does not rely on managerial disclosure or ex-post breach observation, complementing the disclosure-based measures of Florackis et al. (2023), Jiang et al. (2024), Jamilov et al. (2023), and Sheneman (2025), and the breach-event evidence of Campbell et al. (2003), Kamiya et al. (2021), Akey et al. (2021), Makridis (2021), Curti et al. (2023),

and Andreadis et al. (2023). Our measure can be interpreted as a control-environment signal specific to information security, in the spirit of Ashbaugh-Skaife et al. (2009) and Doyle et al. (2007). Second, we provide evidence consistent with cybersecurity exposures being mispriced rather than priced in equity markets, in contrast to the priced-risk findings in disclosure-based studies; the association between exposures and future returns is negative, economically meaningful, and concentrated where investor sophistication is low. Third, we identify two frictions—labor-market tightness and managerial inattention—that are associated with both the persistence of exposures and the magnitude of their valuation consequences, speaking to the broader accounting literature on risk oversight and governance (Ashraf and Sunder, 2023; Kravet and Muslu, 2013).

Our findings should be viewed with three important caveats, which we discuss in detail in the conclusion. First, the measure is restricted to Fortune 500 firms; generalization to smaller, less-resourced firms—where exposures are plausibly more severe—is left to future work. Second, while we document associations between exposures, breaches, profitability, and returns, we cannot fully rule out unobserved firm characteristics that jointly drive exposures and performance. Third, our friction analysis is suggestive rather than causal; pinning down the exact mechanism through which labor scarcity and managerial attention shape cybersecurity outcomes requires more detailed data on firm-level cybersecurity organization and spending.

2 Conceptual Framework

Our novel measure of cybersecurity vulnerabilities is useful if it satisfies two criteria. First, our measure must be correlated with true cybersecurity vulnerabilities. Second, it must contribute novel information about vulnerabilities beyond existing measures in the literature.

To assess the first criterion, we test if our measure of cybersecurity vulnerabilities is associated with future breaches. If our measure is associated with true vulnerabilities, then vulnerable firms under our measure should experience more breaches than non-vulnerable firms.

To assess the second criterion, we conduct asset pricing tests to assess whether cybersecurity vulnerabilities, as measured under our novel measure, are "priced." Cybersecurity vulnerabilities are priced if vulnerable stocks have higher future returns than less vulnerable stocks (Florackis et al., 2023). Such sorting of returns represents compensation to investors for bearing cybersecurity risk, indicating that market participants are aware of cybersecurity vulnerabilities (as measured under our measure). On the other hand, if stocks with high cybersecurity vulnerabilities have lower future returns, this would indicate that the novel measure contains information about realizable risks that is not internalized by market participants.

To test whether vulnerabilities are priced, we follow Florackis et al. (2023) and conduct two related asset pricing tests. First, we sort stocks into high and low vulnerability portfolios. We then form a long-short portfolio by longing the high vulnerability portfolio and shorting the low vulnerability portfolio. We calculate monthly returns for this long-short portfolio

and estimate the following Fama-French 5-Factor Model (Fama and French, 2015):

$$Ret_{p,t} = \alpha + \beta_{MKT} EMRP_t + \beta_{SMB} SMB_t + \beta_{HML} HML_t + \beta_{RMW} RMW_t + \beta_{CMA} CMA_t + \epsilon_{p,t} \quad (1)$$

where EMRP, SMB, HML, RMW, CMA are the market, size, value, investment, and profitability risk factors, respectively. $Ret_{p,t}$ represents monthly excess returns at the portfolio level over the risk-free rate. The parameter of interest is α, which represents excess returns that are not explainable by asset pricing factors. A negative α indicates that cybersecurity risk, as measured under our novel measure, is associated with negative returns not explainable by a standard asset pricing model, suggesting that the risk is not fully priced.

Second, we estimate Fama-MacBeth regressions of individual stock returns on cybersecurity vulnerabilities, controlling for known factors that predict stock returns. Stock returns loading negatively on vulnerabilities would similarly indicate that our measure of cybersecurity risk predicts negative returns and is not fully priced.

3 Data and Measurement

3.1 Background

The vast majority of research on the economics of cybersecurity has focused on publicly reported data breaches, identifying the effects on reputation (Campbell et al., 2003; Spanos and Angelis, 2016; Makridis, 2021; Kamiya et al., 2021; Akey et al., 2021; Florackis et al.,

2023; Andreadis et al., 2023), returns (Johnson et al., 2017), and human capital (Bana et al., 2022). While examining disclosed breaches is a useful exercise, these studies suffer from several important limitations. Reported breaches are non-random because data breaches are either not caught (Makridis and Dean, 2018) or managers decide to under-report them (Amir et al., 2018). Furthermore, some firms and industries are more salient than others and attract more media attention (Makridis et al., 2024). Indeed, the vast majority of breaches do not become public within (Kuypers et al., 2016) or across (Maillart and Sornette, 2010) firms. Data breaches convey useful information, but they are limited for understanding the costs and risks associated with modern computer networks.

To better assess the impact of cybersecurity deficiencies, studies have opted to measure longer-term returns associated with high ex-ante cybersecurity risk as opposed to short-term announcement returns associated with ex-post realized breaches. Examples of this are Florackis et al. (2023) and Jiang et al. (2024), who develop measures of cybersecurity risk using textual analysis of financial statements and track returns for high and low risk firms. This approach benefits from the fact that longer-term returns better capture diminished profitability associated with addressing breaches, even if they are undisclosed. For example, following a breach, a firm may hire a team of cybersecurity specialists, invest in better cybersecurity technologies, and make ransomware payments to hackers to recover lost data. While these costly endeavors are not immediately made public, they will eventually adversely affect profitability and shareholder value.

On the other hand, this approach suffers some drawbacks. First, cybersecurity risk measures are often developed by training textual analysis and machine learning models on the sample of publicly disclosed breaches (Florackis et al., 2023; Jiang et al., 2024; Jamilov

et al., 2023). However, publicly disclosed breaches represent a subset of total breaches that are often less severe (Amir et al., 2018). Second, measures relying on textual analysis of filings and transcripts have difficulties distinguishing between *true* cybersecurity risk and *managerial concern* over cybersecurity risk. Both manifest in greater public discourse on cybersecurity risk, but the latter does not necessarily imply that firms are at greater risk of breaches. In fact, the opposite may be true; firms that express public concern over cybersecurity threats may be more likely to patch exposures.

3.2 A Direct Measure of Cybersecurity Exposures

We take a different approach, drawing on data from Rapid7, a cybersecurity software and advisory firm that provides services to private and public organizations to help strengthen cybersecurity.[4] To facilitate internet-scale telemetry collection of cybersecurity exposures, Rapid7 launched Project Sonar (Galinkin et al. (2022)), an internet scanner building on the work of ZMap (Durumeric et al. (2013)). Rapid7 uses a two-step process by which an initial "probe packet" is sent to all resources on the public internet, and if a response is received, an offline processing of that response attempts to identify the nature of the resource (e.g., firm affiliation).[5]

Resources are identified by an IP address, which identifies a specific machine, and a port number, which identifies an application on that machine. Mapping IP addresses to specific organizations is challenging when scanning the public internet (IPv4 space), as firms are not

[4]Rapid7 makes cybersecurity data available for public research projects through their Open Data portal: https://opendata.rapid7.com/.

[5]Rapid7's collection methodology is comparable to two of the other major internet scanners: Shodan (`https://shodan.io`) and Censys (`https://censys.io/`), differing primarily in scan times and post-processing.

required to register their IP addresses with any public entity. Rapid7 has therefore focused their mapping efforts on large, publicly traded companies in the Fortune 500 to ensure that sample firms are well-known, clearly defined, and have no reason to misdirect those trying to use their legitimate, public-facing resources in a way that, for example, cybercriminals would. In order to perform this mapping, a combination of NetworksDB[6], reverse DNS data, and internet registry information was used. While an inherent limitation of our data is that it does not cover firms outside of the Fortune 500, these firms contribute disproportionately toward US productivity. Moreover, if these firms have cybersecurity exposures, other smaller and less-resourced firms are likely to experience even greater vulnerabilities, on average.

Ultimately, the scans cover more than 100 common ports and protocols across the entirety of the internet in each month.[7] However, certain ports are especially pernicious if exposed to the public internet. Following guidance from Rapid7, we measure a firm's cybersecurity risk as the number of exposed ports in a given firm-month that use Telnet (port number 23), Server Message Block (SMB, port numbers 139 and 445), Secure Shell (SSH, port number 22), and Remote Desktop Protocol (RDP, port number 3389). We term our measure *Cybersecurity Exposures*.

We limit our measure of risk to these four exposure types because they are easy for attackers to detect and target, and straightforward for security teams to mitigate. Telnet is one of the earliest remote login protocols on the internet, released in 1969, that provides a terminal session to the remote host from a client application. However, since there is no encryption in the session between the client and server, anyone with access to the TCP/IP packet flow

[6]https://networksdb.io/

[7]Gathering these externally-collected data on exposed ports has also been shown to dramatically improve the quality of predictions of data breaches and other malicious activity on networks in other contexts (Liu et al., 2015; Zhang et al., 2014).

between the hosts can reconstruct the data, including any usernames and passwords used for logging in. SMB is an internet protocol that allows Windows users to share files. While clients can make SMB requests, and servers can make SMB responses within a network, SMB can also be used over the internet as a protocol to access files on a remote server and other resources (e.g., printers). Since sensitive information is often shared using SMB, SMB ports that are exposed to the public internet carry substantial cybersecurity risk.[8] SSH and RDP are more secure remote administration protocols on the surface. However, they are frequently targeted for brute force attacks and consequently, are common initial access vectors for malicious actors (Beardsley et al. (2022)).

Figure 1 provides an illustrative example of our measurement process for one high-risk port: Telnet. This process is replicated for every high-risk port (Telnet, SMB, SSH, and RDP) every month. Since firms may have multiple open high-risk ports affiliated with many different IP addresses, we calculate *Cybersecurity Exposures* by summing up exposures identified across all high-risk ports within a given firm-month.

Our measure of cybersecurity exposures replicates steps that actual cybercriminals would implement in targeting a firm, without attempting to access firm data. Since our measure is dramatically different from those in the literature, we begin by correlating our measure with a prominent existing cybersecurity risk measure and then validating our measure by examining its breach predictability. We first document that our measure (*Cybersecurity Exposures*) is only *weakly correlated* with that of Florackis et al. (2023). While a regression of Florackis et al. (2023)'s measure on *Cybersecurity Exposures* yields a directionally positive coefficient,

[8] https://blog.rapid7.com/2020/08/21/nicer-protocol-deep-dive-internet-exposure-of-telnet-services/ and https://blog.rapid7.com/2020/09/18/nicer-protocol-deep-dive-internet-exposure-of-smb/

the relation is insignificant at the 10% level.[9] Next, we validate our measure by examining cumulative realized breaches over time for firms with above and below median *Cybersecurity Exposures*. Figure 2 shows that firms with above median exposures experienced over twice as many publicly disclosed cybersecurity breaches over our sample period, suggesting that our direct measure of exposures predicts future breaches and demonstrates the persistent effects of retaining such organizational vulnerabilities.[10]

3.3 Sample and Descriptive Statistics

Our sample is restricted to companies in the Fortune 500 to ensure that IP addresses associated with cybersecurity exposures can be accurately attributed to firms. Cybersecurity exposures and returns are measured at a monthly frequency. Other firm-level characteristics are obtained from the latest 10-K or contemporaneous market data. Our main analysis sample consists of a firm-month panel of public Fortune 500 companies, resulting in 407 unique firms. Our sample timeframe runs from January 2018 through December 2024 and reflects the time series shared with us by Rapid7. The Appendix provides an enumeration of all our variables of interest.

We begin by exploring time series and industry variation in cybersecurity exposures. Figure 3 plots the median number of cybersecurity exposures over time. We find that firms in 2018, the first year in our sample, had the largest number of cybersecurity exposures. Since 2018, cybersecurity exposures have declined in recent years, possibly reflecting greater efforts

[9] We thank Florackis et al. (2023) for providing us with their measure of cybersecurity risk. Our sample and that of Florackis et al. (2023) have only one year of overlap. Therefore, the insignificant correlation may result from a lack of statistical power.

[10] In Section 4, we conduct a more formal statistical analysis corroborating the breach predictability of *Cybersecurity Exposures*.

by firms to address cybersecurity issues. In Figure 4, we find that the four industries with the greatest exposures per firm are Media and Telecommunications (27), Professional Services (13), Food and Accommodations (10), and Warehousing and Couriers (9). In contrast, the four industries with the fewest exposures per firm are Arts and Entertainment (2), Administrative Services (2), Construction (2), and Natural Resource Extraction (2). This is likely a function of their digital intensities: sectors with higher degrees of digitization will naturally have more vulnerabilities (Gallipoli and Makridis, 2018).[11]

In Table 1, we display the distribution of cybersecurity exposures and other firm and stock characteristics. We find that the median firm in our sample has five exposures. Excess returns, measured as a firm's monthly stock return minus the risk-free return, have an interquartile range of -4.9% to 6.2% with a median return of 0.8%. Given that our sample is restricted to public Fortune 500 firms, the market value of sample firms tends to be large. The interquartile range of market capitalization is from $9.2bn to $56.6bn with a median of $22.6bn.[12]

We next examine which firm-level characteristics predict greater cybersecurity exposures. In Table 2 Panel A, we regress logged *Cybersecurity Exposures* on *Size*, *R&D Intensity*, *Profitability*, *B/M* ratios, *Asset Growth*, and *Leverage*. In cross-sectional regressions without (column 1) and with (column 2) industry-month fixed effects, we find that *Size* is positively

[11]The industry distribution of exposures differs from existing measures in the literature. Internet Appendix Figure IA1 displays the industry distribution of cybersecurity risk scores from Florackis et al. (2023). The four industries with the highest and lowest risk scores in Florackis et al. (2023) have no overlap with the highest and lowest exposure industries under our direct measure. Notably, the lowest risk industry from Florackis et al. (2023), Media and Telecommunications, has the highest number of network vulnerabilities.

[12]Internet Appendix Tables IA1 and 2 show the summary statistics by firms with high versus low cyber exposures. The median high-exposure firm has 16 open high-risk ports and a median monthly excess return of 0.676%. Firm size is large, with a median market capitalization of over $30 billion. Notably, these firms exhibit slightly lower profitability (ROA of 0.011) compared to low-exposure firms (ROA = 0.012). Market capitalization is lower than in high-exposure firms, but still substantial, with a median size of $18.8 billion.

associated with *Cybersecurity Exposures*, while *Profitability* and *Asset Growth* are negatively associated with *Cybersecurity Exposures*. However, using a within-firm specification in column 3, we find that higher *B/M* ratios are the only significant predictor of *Cybersecurity Exposures*. Interestingly, the coefficient on *Size* is now negative, albeit insignificantly so.

Inferences are similar when conducting a variance decomposition in Table 2 Panel B. In a cross-sectional regression in columns 1 and 2, *Size* by far is the strongest predictor of *Cybersecurity Exposures*. *Profitability* also explains over 16% of the variation in exposures. However, inferences are substantially different when looking within firm in column 3. With firm fixed effects, *Profitability*, *B/M ratios*, and *Leverage* explain more or similar amounts of variation in exposures compared to *Size*. These results suggest that firms with recent poor financial performance, denoted by weaker profitability, lower market valuations (higher *B/M*), and less debt capacity, tend to invest less in cybersecurity measures. Larger – and perhaps more resourced – firms also appear to better mitigate cybersecurity exposures. Lastly, we note that *Cybersecurity Exposures* is highly persistent within firm. In 41% of observations in our sample, the number of measured exposures remains unchanged compared to the prior month.

4 Cybersecurity Exposures and Stock Returns

This section establishes our main result linking cybersecurity exposures with equity returns. For simplicity, we partition firms into high and low groups based on *Cybersecurity Exposures*.[13] Then, we conduct several exercises to assess whether firms with higher exposures

[13]Internet Appendix Tables IA1 and IA2 display summary statistics for high and low *Cybersecurity Exposure* firms.

exhibit lower future excess returns. We document robustness to alternative expected return models and portfolio constructions, as well as presenting standard cross-sectional Fama-MacBeth regression estimates.

4.1 Univariate Portfolio Sorts

We begin with a portfolio-level analysis of returns. In every month, we assign firms into portfolios of high and low cybersecurity exposures if their exposure count is above and below median, respectively. For each portfolio-month, we calculated equal- and value-weighted excess returns over the following month, where excess returns are computed as monthly equity returns minus the risk-free rate. We are ultimately interested in the differential return of the high exposure portfolio relative to the low exposure portfolio. Therefore, we also calculate returns for long-short portfolios computed as the equal-weighted or value-weighted average return of the high exposure portfolio minus that of the low exposure portfolio.

Table 3 presents the results of these univariate portfolio sorts. We start by examining excess returns. The equal-weighted average monthly excess return for the low exposure portfolio is 1.10%, compared to 0.77% for the high exposure portfolio. The long-short (high minus low exposure) portfolio has a statistically significant excess return of -0.33%. Similar results obtain when portfolio returns are calculated by value-weighting. The value-weighted average monthly excess return of the low exposure portfolio is 1.89%, compared to 1.11% for the high exposure portfolio. The long-short portfolio has a statistically significant excess return of -0.78%.

To account for the possibility that excess returns are driven by exposure to various market

factors, we present portfolio alphas calculated from a Fama-French 5-Factor Model (Fama and French (2015)). Specifically, alphas are adjusted for market risk, size, book-to-market ratios, profitability, and investment. The alpha for the long-short portfolio is -0.38% when excess returns are calculated on an equal-weighted basis and -0.68% when excess returns are calculated on a value-weighted basis. In both cases, estimated alphas are statistically significant at the 5% level.

4.2 Robustness and Bivariate Portfolio Sorts

To provide confidence that our results are robust, we consider alternative expected return models to calculate alphas. In Table 4, we calculate alpha using the CAPM model (Sharpe (1964)), Fama-French 3-Factor Model (Fama and French (1993)), and Carhart 4-Factor Model (Carhart (1997)). Under these alternative expected return models, estimated alphas from the long-short portfolio continue to remain negative and significant with magnitudes between -0.30% and -0.73%.

We also provide evidence that our results are not driven by noise in the measurement of cybersecurity exposures. In the last two rows of Table 4, we sort firms into high and low exposure portfolios based on a six-month rolling average measure of exposures, smoothing out noise in any given month. We find that results obtain when forming portfolios based on rolling average exposures. Estimated alphas, calculated under a 5-Factor Model, are a statistically significant -0.30% under equal-weighting and -0.49% under value-weighting.

Next, we conduct a series of portfolio double sorts to see if our high-low portfolio performance is driven by factors known to explain returns, such as size and book-to-market (Fama

and French, 1993). Table 5 shows 5-Factor alphas for long-short portfolios sorted on an additional characteristic. Rows 1 and 2 report long-short alphas for below and above median market capitalization firms, respectively. For low and high *Size* firms, we find that negative and significant alphas persist under both equal-weighted and value-weighted portfolios with magnitudes ranging from -0.31% to -0.74%. Similarly, rows 3 and 4 report long-short alphas for below and above median book-to-market ratio firms, respectively. For both low and high *B/M* firms, we estimate negative alphas under both equal-weighted and value-weighted portfolios with magnitudes ranging from -0.28% to -0.91%. While we do not estimate significant alphas in all double-sorted portfolios, significance does not solely concentrate in either of the low or high *B/M* portfolios, suggesting *B/M* does not solely explain cybersecurity exposure alphas.

4.3 Fama-MacBeth Regressions

We now turn to stock-level analyses exploiting cross-sectional variation in firm characteristics in a Fama-MacBeth regression framework (Fama and MacBeth, 1973). These regressions allow us to control for firm-specific characteristics that may explain stock returns. Following Florackis et al. (2023), in Table 6 we control for beta, size, and book-to-market ratios (Fama and French, 1993), momentum (Jegadeesh and Titman, 1993), short-term reversals (Jegadeesh, 1990), idiosyncratic volatility (Ang et al., 2006), illiquidity (Amihud, 2002), coskewness (Harvey and Siddique, 2000), max stock price (Bali et al., 2011), asset growth and ROA (Fama and French, 2015), and R&D expenditures (Hirshleifer et al., 2013). Our independent variable of interest is *High Exposures*, an indicator variable taking the value one

(zero) if a firm has above (below) median cybersecurity exposures.

We begin in column 1 with a parsimonious model of returns one month ahead regressed on only *High Exposures*. We find that high cybersecurity exposures are associated with a -0.33 percentage point decrease in excess returns, a relation that is statistically significant and of similar magnitude as our portfolio-level analyses. In column 2, we include controls for beta, size, and book-to-market ratios and continue to find a negative and significant return differential between high and low cybersecurity exposure firms. Results obtain with the inclusion of controls for momentum, short-term reversals, idiosyncratic volatility, illiquidity, coskewness, and max stock price in column 3. Lastly, we continue to find a negative and significant coefficient on *High Exposures* with the inclusion of firm-level characteristics such as ROA, asset growth, and R&D intensity. Overall, these results provide cross-sectional validation of our main finding that greater cybersecurity exposures are associated with lower future excess returns.[14,15]

Finally, we conduct a horse race between our measure and that from Florackis et al. (2023) in Table IA5 in the Internet Appendix. Crucially, when we control for both our measure of whether the company ranks above the median in cyber exposures and the Florackis et al. (2023) measure, only ours is significant, suggesting that exposed ports within a company capture a different dimension of asset prices than the traditional exposure measure.

[14]Table IA3 in the Internet Appendix examines whether there is heterogeneity over time. The negative association is concentrated in 2020–2021 (coefficient = -0.471, $p<0.05$), while it is weaker and less statistically significant in the other years. This is consistent with a rise of vulnerabilities, particularly during an era of intense remote work when individuals may have been more susceptible to ransomware and phishing attacks.

[15]We consider additional robustness to address concerns that industry-level trends in returns during our analysis period are driving our findings. In Table IA4, we add industry fixed effects to our baseline Fama-MacBeth analysis to control for average industry-level returns and continue to find lower returns in high cybersecurity exposure stocks. While our results are robust to the inclusion of industry fixed effects, we refrain from using this specification as our baseline since fixed effects heavily restrict degrees of freedom when estimating regressions in the time series.

The absence of significance on their measure, however, does not imply that it is not important; quite the contrary, after controlling for actual (supply-side) vulnerabilities, the way companies communicate information in their financial statements does not have additional predictive power on asset prices.

5 Mechanisms

In this section, we explore the economic mechanisms underlying the underperformance of high exposure stocks. We first link exposures to breaches, which are associated with negative announcement returns and loss of profitability. We next ask why cybersecurity risk, when directly measured as network vulnerabilities, is not priced. Lastly, we explore why firms leave exposures unaddressed if they are so pernicious for shareholder value.

5.1 Exposures as Predictors of Realized Breaches

Several studies have documented that breach disclosures are associated with negative announcement returns (Kamiya et al., 2021; Akey et al., 2021). Therefore, the underperformance of high cybersecurity exposure firms may plausibly be attributable to realized cybersecurity breaches. We explore this idea in this section, which also serves as validation for our measure.

We begin in Table 7 by documenting that cybersecurity exposures are predictive of extreme three standard deviation drops in stock prices. The results are robust to firm and industry-month fixed effects, as well as controls for firm and stock characteristics used in prior Fama-MacBeth regressions. The association is economically meaningful: a one hundred

percent increase in (doubling of) cybersecurity exposures is associated with a 0.2 percentage point increased likelihood of an extreme negative return over the following month, representing a material increase relative to the unconditional extreme negative return probability of 0.8%.[16]

Furthermore, these extreme negative returns over the following month are attributable to realized cybersecurity breaches. In Table 8, we find that cybersecurity exposures are associated with greater likelihood of a realized cybersecurity breach over the following quarter. The results obtain when controlling for time-varying industry-wide trends in cybersecurity attacks (industry-month fixed effects), unobservable cross-sectional differences in breach probability (firm fixed effects), time-varying firm characteristics that are associated with cybersecurity, such as firm size, R&D expenditures, ROA, B/M ratios, and growth, as well as the controls used in the cross-sectional Fama-MacBeth regressions in Table 6. In terms of economic magnitude, a a one hundred percent increase in cybersecurity vulnerabilities is associated with a 0.7 percentage point increase in breach probability one quarter in the future. The elevated breach risk is economically meaningful when considering that the unconditional one quarter breach probability is 1.4%.

A drawback of the above analysis is that data on cybersecurity breaches come from firms' public disclosures. Amir et al. (2018) find that many cybersecurity breaches are undisclosed, and undisclosed breaches tend to be costlier for firms upon discovery (e.g., via whistleblowers). However, even undisclosed breaches require costly remediation efforts from

[16]Table IA6 in the Internet Appendix assesses whether cybersecurity exposures are associated with a higher likelihood of extreme positive stock returns (defined as 3σ-above-mean). Across all specifications, the coefficient on log(Cybersecurity Exposures) is effectively zero and statistically insignificant. The lack of any significant positive association between exposures and tail-upside events is consistent with a causal story where vulnerabilities create significant downside risk.

firms. Following a breach, firms may need to hire cybersecurity professionals and invest in information security technologies. Firms may even have to pay a "ransom" in the event of a ransomware attack. While the average payment per ransomware incident in 2023 was $1.5mm, payments can be much larger. In 2021, CNA Financial made the largest (publicly known) ransomware payment of $40mm.

Next, we study whether cybersecurity exposures are associated with reduced profitability in Table 9. In firm-quarter level regressions, we find that a a one hundred percent increase in average cybersecurity exposures over a quarter predicts a 10 basis point decrease in profitability in the following quarter, where profitability is measured as EBITDA divided by total assets. The results are robust to controlling for firm and industry-quarter fixed effects (column 1), firm characteristics (column 2), and lagged profitability (column 3).

5.2 Why Are Exposures Not Priced?

Prior studies measuring cybersecurity risk using models built on textual and financial data have found that cybersecurity is priced in equity markets. Jiang et al. (2024) and Florackis et al. (2023) find greater cybersecurity risk under their respective measures predicts positive future returns. However, using similar portfolio sorting and Fama-MacBeth analyses, we uncover a different result. Firms with greater cybersecurity risk, when directly measured as exploitable exposures in a firm's network infrastructure, experience negative future returns. This finding suggests that equity markets are not properly pricing cybersecurity exposures, even though exposure measurement is conducted using publicly accessible information and tools.

Here, we analyze why cybersecurity exposures are not priced by investors. We hypothesize that reproducing our measure of cybersecurity exposures requires sophisticated knowledge of cybersecurity, programming, and computer networks that is not common among investors. According to data from the American Community Survey from 2018 to 2024, under 2% of workers in finance occupations have a degree in computer or information sciences, where finance occupations are defined as SOC codes from 132000-132099 and 113031. This likely represents an extreme upper bound estimate of the share of investors that can identify cybersecurity exposures, since only a small subset of computer and information science graduates have cybersecurity-specific knowledge. Therefore, only the most sophisticated investors could potentially identify and trade on exposures.

We test this idea in Table 10 by estimating 5-Factor alphas for long-short portfolios sorted on both cybersecurity exposures and investor sophistication. We measure investor sophistication as one minus the share of investors that are index investors. Our measure is based on Coles et al. (2022), who find that passive index investors tend to be less informed, suggesting that a lower share of index investors is associated with greater investor sophistication. Rows 1 and 2 report long-short alphas for stocks with below and above median investor sophistication, respectively. For stocks with low investor sophistication, we estimate negative and significant -0.57% and -0.81% monthly alphas under an equal-weighted and value-weighted portfolio, respectively. Overall, the double-sort analysis suggests that negative returns concentrate in stocks with low investor sophistication.

Similar inferences obtain in cross-sectional Fama-MacBeth regressions in Internet Appendix Table IA7. We replicate the specifications in Table 6 except our coefficient of interest is *High Exposures* $\times$ *Low Investor Sophistication*, which captures the differential excess return

for low investor sophistication stocks in the face of high cybersecurity exposures. We find generally negative and significant coefficient estimates on *High Exposures* × *Low Investor Sophistication*, suggesting that cybersecurity exposures are more negatively associated with returns when investors are relatively unsophisticated. Both the Fama-MacBeth and double sort analyses show that negative returns concentrate where investors are less likely to identify and trade on cybersecurity exposures.

5.3 Why Are Exposures Unaddressed by Firms?

Given that exposures are costly in terms of profitability and shareholder value for firms, we next explore why exposures are allowed to persist. Leaving cybersecurity exposures unaddressed does not appear to be an optimal policy, since the median expected loss in shareholder value is approximately $75mm over the following month for our sample firms. Furthermore, we find that the correlation between *Cybersecurity Exposures* in month t and $t+1$ is 95.5%, suggesting that cybersecurity exposures that exist in one month are likely to persist into the following month. These facts point to the existence of potential frictions that prevent firms from eliminating exposures in a timely manner, thereby reducing their liabilities.

One source of frictions may arise from labor shortages among cybersecurity professionals, which inhibit firms from patching cybersecurity exposures. The latest estimates suggest that 265,000 cybersecurity workers are needed (Lightcast, 2024). To put that in perspective, 2024 alone had 457,433 openings with cybersecurity-related skills, according to CyberSeek.org.[17]

[17] https://www.cyberseek.org/

Using data from the ACS, we measure a firm's exposure to cybersecurity labor market tightness as the annual growth in residual salary for cybersecurity professionals (defined as SOC code = 151212, "Information Security Analyst") in the firm's headquarters state (*Cybersecurity Labor Tightness*), obtained by taking the residuals from a regression of logged salary on age, education, sex, and race, isolating the portion of wages that could be considered as unobserved human capital. We use wage growth to proxy for labor shortages because wage growth has historically been associated with a host of supply-side and demand-side indicators of labor market tightness (e.g., unemployment rates and job vacancies) (Domash and Summers, 2022).

We begin by documenting several stylized facts about cybersecurity labor market tightness. In Internet Appendix Figure IA2, we find that *Cybersecurity Labor Tightness* is positively and significantly correlated with cybersecurity exposures. In Internet Appendix Figure IA3, we find that exposures are more likely to translate into realized breaches when cybersecurity talent is costly to acquire. In Panel A, we find that the one-month breach probability for high exposure firms is 1.3x that of low exposure firms when firms have low (below median) *Cybersecurity Labor Tightness*. However, for firms facing high (above median) *Cybersecurity Labor Tightness*, the one-month breach probability for high exposure firms is 3.0x that of low exposure firms. Similar results obtain when examining three-month breach probability in Panel B. These findings suggest that difficulties in hiring cybersecurity professionals are associated with the quantity of exposures and the probability that exposures manifest into realized breaches.

Next, we consider the impact of cybersecurity labor market tightness on equity returns to exposures. In Table 11, we estimate 5-Factor alphas for long-short portfolios sorted on both

cybersecurity exposures and *Cybersecurity Labor Tightness*. Rows 1 and 2 report long-short alphas for firms with below and above median *Cybersecurity Labor Tightness*, respectively. For firms with high *Cybersecurity Labor Tightness*, we estimate negative and significant -.76% and -1.28% monthly alphas under equal-weighted and value-weighted portfolios, respectively. We find less negative and insignificant alphas for firms with low *Cybersecurity Labor Tightness*. Similar inferences obtain in the cross-section of individual stocks. In Internet Appendix Table IA8, we conduct Fama-MacBeth regressions and find negative and significant coefficient estimates on *High Exposures* × *High Cybersecurity Labor Tightness*. In the most robust specification (column 4), we find that returns for high exposure firms are lower by -0.38 percentage points when firms also face tight cybersecurity labor markets. These findings suggest that labor shortages among cybersecurity professionals hamper firms' ability to patch exposures, which ultimately adversely affect equity returns.

However, labor shortages are unlikely to be the full explanation for unaddressed exposures. After all, if cybersecurity exposures are expected to cost the median Fortune 500 firm $75mm over the following month, then this firm should in theory be willing to pay up to $75mm for workers, enough to entice most cybersecurity professionals to work for a firm. We propose that managerial inattention to cybersecurity represents another friction inhibiting firms from addressing cybersecurity exposures in a timely manner. Since cybersecurity is outside of the core business of our sample firms, executives with limited attention are unlikely to focus on cybersecurity unless some event draws their attention (Dessein et al. (2016); Dessein and Santos (2021)). Consistent with existing literature, we propose that firms focus more on addressing cybersecurity exposures following cybersecurity breaches (Bana et al. (2022)).[18]

[18] Bana et al. (2022) find that firms hire more cybersecurity professionals following cybersecurity breaches.

We define a firm to have high (low) *Cybersecurity Attention* if it (did not) experienced a cybersecurity breach in the past five years.

We first document in Internet Appendix Figure IA4 that high *Cybersecurity Attention* firms have less than half the exposures of low *Cybersecurity Attention* firms. A drawback to using breach history as a proxy of cybersecurity attention is that breach data is voluntarily disclosed. In reality, many breaches may be unknown to the public. Nevertheless, public breaches predict tangible changes in firms' cybersecurity policies. In Internet Appendix Figure IA5, we find that 23.1% of firms with high *Cybersecurity Attention* have a chief information security officer (CISO) on the board, almost twice the rate of low *Cybersecurity Attention* firms, suggesting that public breaches motivate shareholders to appoint directors with cybersecurity expertise and focus.

We next examine the impact of cybersecurity attention on equity returns to exposures. In Table 12, we estimate 5-Factor alphas for long-short portfolios sorted on both cybersecurity exposures and *Cybersecurity Attention*. Rows 1 and 2 report long-short alphas for firms with low and high *Cybersecurity Attention*, respectively. A long-short strategy on exposures for low *Cybersecurity Attention* stocks exhibits negative and significant -0.42% and -0.74% monthly alphas under equal-weighted and value-weighted portfolios, respectively. High *Cybersecurity Attention* stocks on the other hand exhibit insignificant alphas. In cross-sectional Fama-MacBeth regressions (Inernet Appendix Table IA9), we similarly find returns to be more negative in low *Cybersecurity Attention* stocks. These findings show that attention to cybersecurity issues, or lack thereof, impacts cybersecurity exposures and ultimately shareholder value. Of note, the media plays a major role in propagating these shocks by altering the salience; for instance, prior work has looked at how the media differentially treats data

breaches based on the size and sector (Makridis, 2021; Makridis et al., 2024).

Some of these agency problems could arise internally within organizations. For example, if the chief financial officer (CFO) or chief marketing officer (CMO) wields more power than the chief information security officer (CISO), potentially due to the relative ease of observing their metrics over the CISO, then that could cause a delinquency in cybersecurity improvements. For example, a 2022 survey by FTI Consulting found that "66% of CISOs felt senior leadership struggles to fully understand their role within the organization, whereas 31% of C-suite executives expressed difficulty understanding the tangible return on cybersecurity investment."[19] Furthermore, a 2024 survey by IANS Research found that "75% of them [CISOs] said they are looking for a job change" and that "while more than 63% of CISOs have a vice president or director-level position, only 20% are at the C-suite level despite having "chief" in their title."[20] Agency problems could also arise due to inadequate regulatory clarity. For instance, Shackelford et al. (2022) discuss how the Department of Justice has requested organizations adhere to "reasonable cybersecurity" measures, but no such definition of reasonable cybersecurity exists.

6 Conclusion

While cybersecurity has become a growing threat to economic prosperity, we know little about how to measure cybersecurity exposures, the cross-section of such exposures across firms, and whether they matter for firm value. We measure cybersecurity exposures by simulating port scan attacks and counting the number of publicly accessible vulnerable ports

[19]Source: FTI Consulting
[20]Source: Darkreading

for Fortune 500 firms. We show that high exposure firms exhibit negative excess returns relative to low exposure firms. The estimated underperformance amounts to 0.33% per month, or approximately $75mm in value lost for the median size firm in the Fortune 500. We investigate the mechanisms behind these results. We find that exposures predict subsequent breach disclosures, future sharp declines in stock returns, and lower profitability in the following quarter. While much more work is needed to be sure, we provide some evidence that cybersecurity exposures are not priced because investors lack sophistication to identify and take advantage of exposures. Furthermore, firms are not able to address exposures due to a scarcity of cybersecurity professionals and limited managerial attention towards cybersecurity. In sum, we provide a new method of identifying cybersecurity exposures, measure the cost of these exposures to shareholders, and offer evidence that frictions hamper identification of exposures by investors and remediation of exposures by firms.

Our work nonetheless leaves a handful of questions for further research. First, since cybersecurity is a multi-dimensional concept, we would like to benchmark our proxies for vulnerabilities with other measures. Second, while we offer some evidence about frictions that contribute to the persistence in these vulnerabilities, we cannot causally pinpoint the source or exact mechanism. Future work should leverage more detailed labor market data on employment and skills to see whether the companies with greater vulnerabilities are also those that chronically fail to attract cyber and cyber-adjacent workers. Third, if there are frictions that contribute to the mispricing of cybersecurity, then are there public policy tools that could help ameliorate these frictions? We leave these questions to future work, and continue to encourage improved measurement of cybersecurity vulnerabilities for not only publicly traded companies, but also private ones.

References

Akey, P., Lewellen, S., Liskovich, I., and Schiller, C. (2021). Hacking corporate reputation. *Working Paper*.

Amihud, Y. (2002). Illiquidity and stock returns: cross-section and time-series effects. *Journal of Financial Economics*, 5(1):31–56.

Amir, E., Levi, S., and Livne, T. (2018). Do firms underreport information on cyber attacks? Evidence from capital markets. *Review of Accounting Studies*, 23:1177–1206.

Andreadis, L., Kalotychou, E., Louca, C., Lundblad, C., and Makridis, C. A. (2023). From Bits to Bonds: The Economic Ripple of Local Cyberattacks on Municipalities. *SSRN working paper*.

Ang, A., Hodrick, R. J., Xing, Y., and Zhang, X. (2006). The cross-section of volatility and expected returns. *Journal of Finance*, 61(1):259–299.

Ashbaugh-Skaife, H. A., Collins, D. W., Kinney Jr., W. R., and LaFond, R. (2009). The effect of SOX internal control deficiencies on firm risk and cost of equity. *Journal of Accounting Research*, 47(1):1–43.

Ashraf, M. and Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review*, 98(4):1–32.

Bali, T. G., Cakici, N., and Whitelaw, R. F. (2011). Maxing out: Stocks as lotteries and the cross-section of expected returns. *Journal of Financial Economics*, 99(2):427–446.

Bana, S., Brynjolfsson, E., Jin, W., Steffen, S., and Wang, X. (2022). Human capital acquisition in response to data breaches. *SSRN working paper*.

Beardsley, T., Galinkin, E., and Barnard, C. (2022). Good passwords for bad bots. *Rapid7 Technical Report*, pages 1–2.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431–448.

Carhart, M. (1997). On persistence in mutual fund performance. *Journal of Finance*, 52(1):57–82.

CEA (2019). Economic Report of the President. *The White House Council of Economic Advisers*.

Coles, J. L., Heath, D., and Ringgenberg, M. C. (2022). On index investing. *Journal of Financial Economics*, 145(3):665–683.

Collins, D. W., Gong, G., and Hribar, P. (2003). Investor sophistication and the mispricing of accruals. *Review of Accounting Studies*, 8(2-3):251–276.

Condon, C., Galinkin, E., and Bowes, R. (2023). 2023 vulnerability intelligence report. *Rapid7 Technical Report*.

Curti, F., Ivanov, I., Macchiavelli, M., and Zimmermann, T. (2023). City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity. *SSRN working paper*.

Cybersecurity and Infrastructure Security Agency (2022). Bod 23-01: Improving asset visibility and vulnerability detection on federal networks. Technical report, CISA.

Dessein, W., Galeotti, A., and Santos, T. (2016). Rational inattention and organizational focus. *American Economic Review*, 106(6):1522–1536.

Dessein, W. and Santos, T. (2021). Managerial style and attention. *American Economic Journal: Microeconomics*, 13(3):372–403.

Dhaliwal, D., Judd, J. S., Serfling, M., and Shaikh, S. (2016). Customer concentration risk and the cost of equity capital. *Journal of Accounting and Economics*, 61(1):23–48.

Domash, A. and Summers, L. H. (2022). How tight are U.S. labor markets? *Working Paper*.

Doyle, J. T., Ge, W., and McVay, S. (2007). Accruals quality and internal control over financial reporting. *The Accounting Review*, 82(5):1141–1170.

Durumeric, Z., Wustrow, E., and Halderman, J. A. (2013). Zmap: Fast internet-wide scanning and its security applications. In *USENIX Security Symposium*, volume 8, pages 47–53.

Fama, E. F. and French, K. R. (1993). Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics*, 33(1):3–56.

Fama, E. F. and French, K. R. (2015). A five-factor asset pricing model. *Journal of Financial Economics*, 116(1):1–22.

Fama, E. F. and MacBeth, J. D. (1973). Risk, return, and equilibrium: Empirical tests. *Journal of Political Economy*, 81(3):607–636.

Florackis, C., Louca, C., Michaely, R., and Weber, M. (2023). Cybersecurity risk. *Review of Financial Studies*, 36(1):351–407.

Galinkin, E., Beardsley, T., and Deardorff, P. (2022). Open data: Internet scale telemetry. *Rapid7 Technical Report*.

Gallipoli, G. and Makridis, C. A. (2018). Structural Transformation and the Rise of Information Technology. *Journal of Monetary Economics*, 97:91–110.

Harvey, C. R. and Siddique, A. (2000). Conditional skewness in asset pricing tests. *Journal of Finance*, 55(3):1263–1295.

Hirshleifer, D., Hsu, P.-H., and Li, D. (2013). Innovative efficiency and stock returns. *Journal of Financial Economics*, 107(3):632–654.

Jamilov, R., Rey, H., and Tahour, A. (2023). The anatomy of cyber risk. *Working Paper*.

Jegadeesh, N. (1990). Evidence of predictable behavior of security returns. *Journal of Finance*, 45(3):881–898.

Jegadeesh, N. and Titman, S. (1993). Returns to buying winners and selling losers: Implications for stock market efficiency. *Journal of Finance*, 48(1):65–91.

Jensen, M. C. and Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4):305–360.

Jiang, H., Khanna, N., Yang, Q., and Zhou, J. (2024). The cyber risk premium. *Management Science*, 70(12):8791–8817.

Johnson, M. S., Kang, M. J., and Lawson, T. (2017). Stock price reaction to data breaches. *Journal of Financial Issues*, 16:1–13.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., and Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3):719–749.

Kravet, T. and Muslu, V. (2013). Textual risk disclosures and investors' risk perceptions. *Review of Accounting Studies*, 18(4):1088–1122.

Kuypers, M., Maillart, T., and Pate-Cornell, E. A. (2016). An empirical analysis of cyber security incidents at a large organization. *Workshop on the Economics of Information Security*.

Leuz, C. and Wysocki, P. D. (2016). The economics of disclosure and financial reporting regulation: Evidence and suggestions for future research. *Journal of Accounting Research*, 54(2):525–622.

Lightcast (2024). The Lightcast Quarterly Cybersecurity Talent Report. *Lightcast*.

Liu, Y., Sarabi, A., Zhang, J., Naghizadeh, P., Karir, M., Bailey, M., and Liu, M. (2015). Cloudy with a chance of breach: Forecasting cyber security incidents. *Proceedings of the 24th USENIX Security Symposium, Washington DC*.

Maillart, T. and Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *European Physical Journal*, 75:357–364.

Makridis, C. A. (2021). Do data breaches damage reputation? Evidence from 43 companies between 2002 and 2018. *Journal of Cybersecurity*, 7(1).

Makridis, C. A. and Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. *Journal of Economic and Social Measurement*, 43:59–83.

Makridis, C. A., Maschmeyer, L., and Smeets, M. (2024). If it bleeps it leads? - Media coverage on cyber conflict and misperception. *Journal of Peace Research*, 6(1).

PwC (2017). 20th Annual Global CEO Survey. *PwC Global*.

Rapid7 (2020). National / industry / cloud exposure report (nicer) 2020. Technical report, Rapid7.

Shackelford, S., Boustead, A., and Makridis, C. A. (2022). Defining "Reasonable Cybersecurity": Evidence from the States. *Yale Journal of Law and Technology*.

Sharpe, W. F. (1964). Capital asset prices: A theory of market equilibrium under conditions of risk. *Journal of Finance*, 19(3):425–442.

Sheneman, A. (2025). Cybersecurity risk and bank loan contracting. *The Accounting Review*, pages 1–25.

Spanos, G. and Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58:216–229.

Verizon (2024). 2024 data breach investigations report. Technical report, Verizon Business.

WEF (2017). Global risks report 2017. *World Economic Forum*.

Zhang, J., Durumeric, Z., Bailey, M., Liu, M., and Karir, M. (2014). On the mismanagement and maliciousness of networks. *NDSS Symposium 2014*.

Tables and Figures

Figure 1

Measurement of Cybersecurity Exposures

This figure illustrates the measurement of cybersecurity exposures for one high risk port: Telnet (port number 23). This procedure is replicated for all other high risk ports. *Cybersecurity Exposures* measures the total number of exposures across all high risk ports (Telnet, SMB, SSH, and RDP), in a given firm-month.

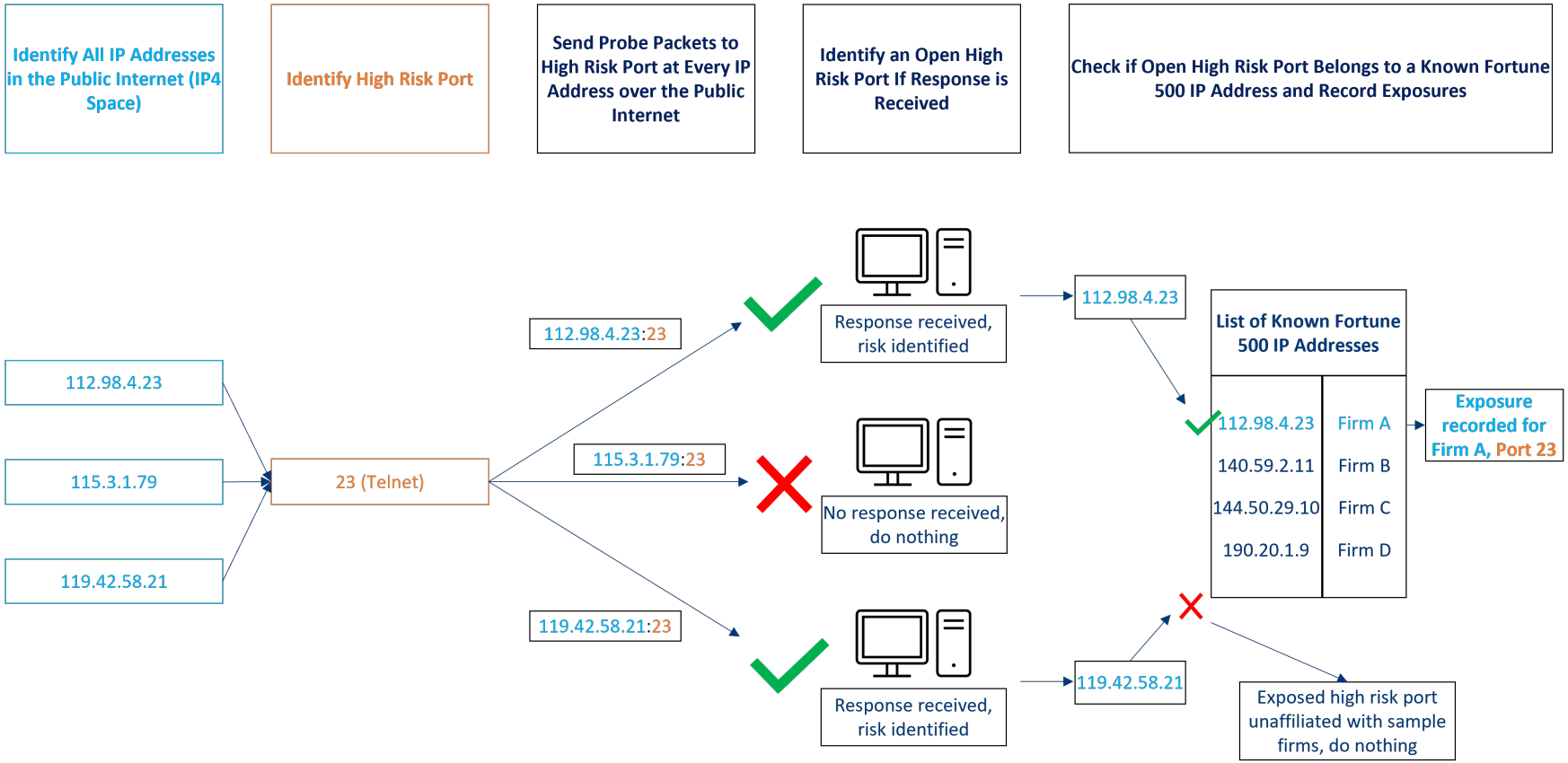

Figure 2

Cybersecurity Breaches by Exposures

This figure displays the cumulative number of cybersecurity breaches by high and low cybersecurity exposures. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The sample is further restricted to firms with data on cybersecurity breaches, where our breach data sample ends in 2021. *High (Low) Exposure* is defined as having above (below) median *Cybersecurity Exposures*. Detailed variable descriptions can be found in the Appendix.

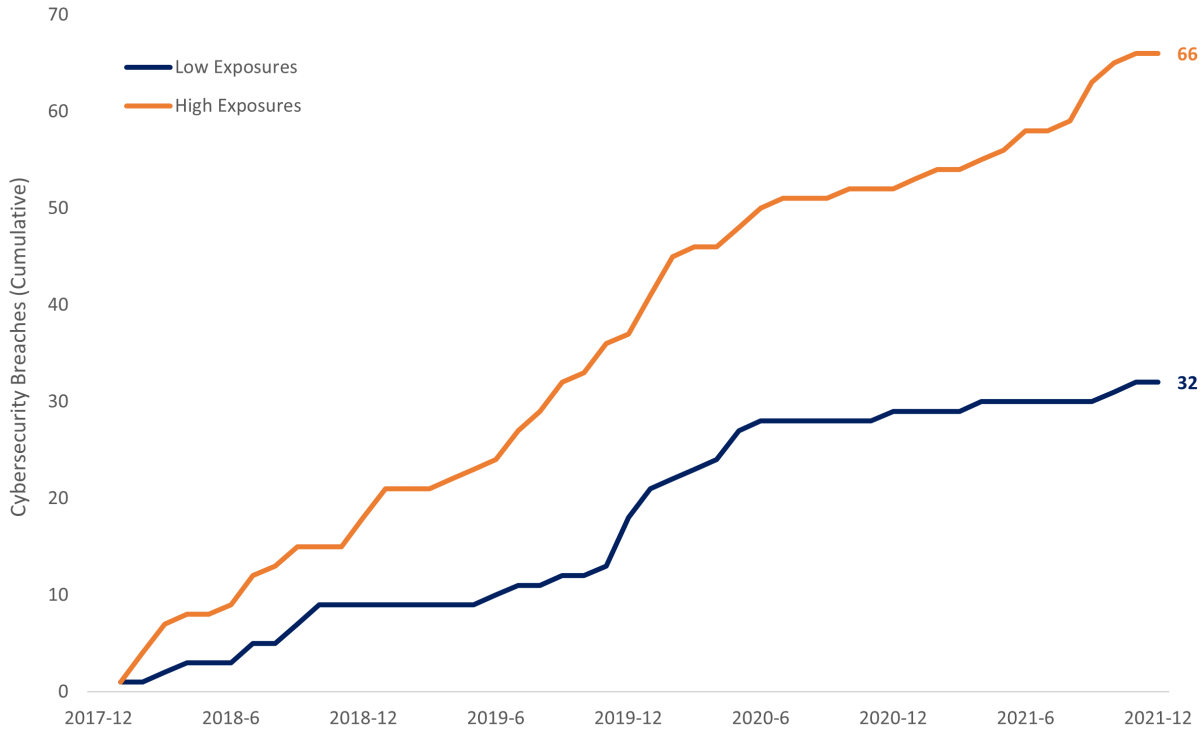

Figure 3

Cybersecurity Exposures over Time

This figure displays the median number of cybersecurity exposures by year. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Detailed variable descriptions can be found in the Appendix.

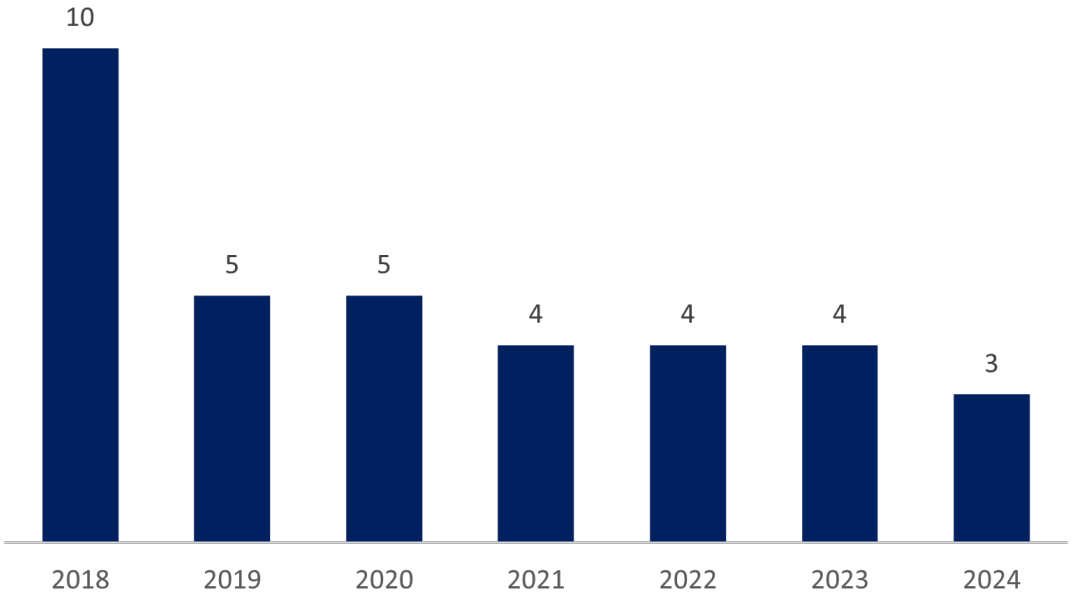

Figure 4

Cybersecurity Exposures by Industry

This figure displays median cybersecurity exposures by industry. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Industry is defined by 2-digit NAICS codes, where 2-digit NAICS codes are displayed in parentheses beside the industry name. Detailed variable descriptions can be found in the Appendix.

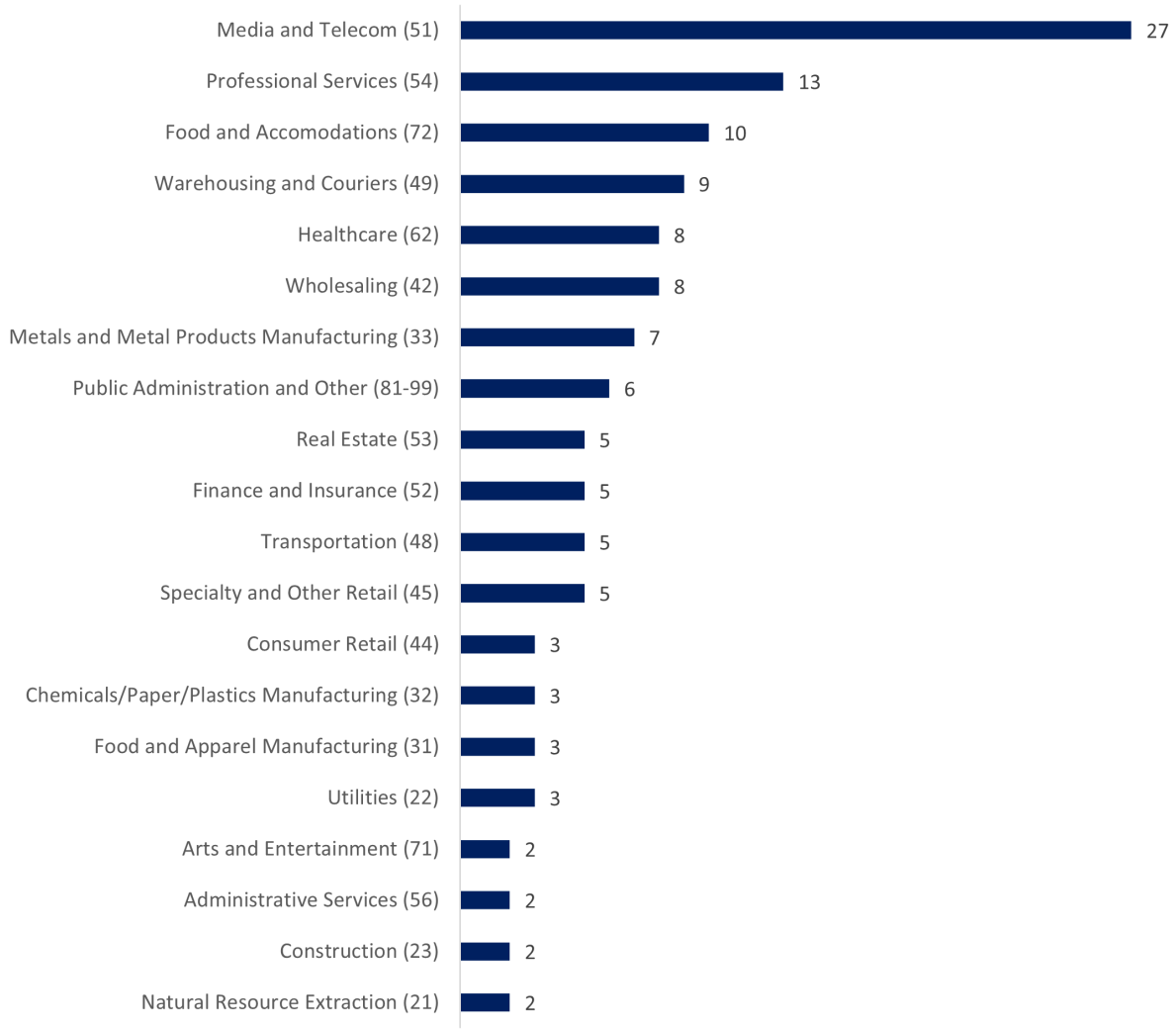

Table 1
Descriptive Statistics

This table displays descriptive statistics of key variables. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Detailed variable descriptions can be found in the Appendix.

	Percentile		
	25th	50th	75th
	(1)	(2)	(3)
Cybersecurity Exposures	0.000	5.000	15.000
Excess Return (%)	-4.923	0.755	6.232
Size (Market Cap, USD mm)	9232.294	22611.072	56586.773
B/M	0.164	0.370	0.660
Profitability	0.018	0.028	0.041
ROA	0.004	0.011	0.022
Asset Growth	-0.011	0.008	0.029
R&D Intensity	0.000	0.000	0.000
Leverage	0.224	0.350	0.459
Beta	0.773	1.097	1.430
Momentum	0.911	1.086	1.281
Reversal	-4.923	0.755	6.232
Idiosyncratic Volatility	0.045	0.056	0.075
Illiquidity	-0.001	0.000	0.001
CoSkew	-0.030	0.002	0.038
Max Stock Price	44.836	82.922	150.578
Investor Sophistication	0.416	0.500	0.583
Cybersecurity Labor Tightness	-0.069	0.016	0.139

Table 2
Determinants of Cybersecurity Exposures

This table displays multivariate regressions (Panel A) and the corresponding variance decomposition (Panel B) of cybersecurity exposures on firm-level characteristics. The dependent variable is the logarithm of *Cybersecurity Exposures*, and regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Standard errors are reported in brackets and clustered at the firm level. The figures displayed in the variance decomposition in Panel B represent the fraction of type III sum of squared errors. We exclude fixed effects from our calculation of total type III sum of squared errors. Detailed variable descriptions can be found in the Appendix. (*** p<0.01, ** p<0.05, * p<0.10)

Panel A: Multivariate Regressions

	ln(Cybersecurity Exposures)		
	(1)	(2)	(3)
Size	.174***	.243***	-.050
	[.051]	[.063]	[.084]
R&D Intensity	10.295	6.430	2.238
	[7.758]	[7.296]	[1.572]
Profitability	-5.455***	-7.204***	-1.203
	[1.997]	[2.268]	[1.143]
B/M	-.000	.003	.010*
	[.015]	[.015]	[.005]
Asset Growth	-.493***	-.512***	-.058
	[.169]	[.197]	[.096]
Leverage	.099	.408	.338
	[.303]	[.342]	[.445]
Firm FE	No	No	Yes
Ind-Month FE	No	Yes	Yes
Observations	26177	25978	25978
R-squared	.03	.17	.74

Table 2
Determinants of Cybersecurity Exposures (Continued)

Panel B: Variance Decomposition

(*** p<0.01, ** p<0.05, * p<0.10)

	ln(Cybersecurity Exposures)		
	(1)	(2)	(3)
Size	0.699	0.758	0.184
R&D Intensity	0.090	0.019	0.089
Profitability	0.174	0.164	0.249
B/M	0.000	0.000	0.153
Asset Growth	0.033	0.022	0.031
Leverage	0.004	0.036	0.294
Firm FE	No	No	Yes
Ind-Month FE	No	Yes	Yes

Table 3
Returns by Cybersecurity Exposure Portfolios

This table displays equal- and value-weighted average excess returns and five-factor alphas (Fama and French (2015)) by cybersecurity exposure portfolios. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Returns are calculated as cum-dividend monthly returns. Stocks are sorted into *High (Low) Exposure* portfolios if their cybersecurity exposures are above (below) median in a given month. Portfolio returns are tracked over the following month, and portfolios are rebalanced on a monthly basis. A Long-short portfolio is formed in column (3) by going long on the *High Exposure* portfolio (column (2)) and shorting the *Low Exposure* portfolio (column (1)). Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Low Exposures	High Exposures	Long-Short (H-L)
	(1)	(2)	(3)
Excess Returns			
Equal-Weighted	1.093*	.767	-.326**
	[.657]	[.619]	[.156]
Value-Weighted	1.888***	1.106**	-.783***
	[.549]	[.506]	[.265]
5-Factor Alpha			
Equal-Weighted	.172	-.204*	-.375**
	[.161]	[.120]	[.159]
Value-Weighted	.886***	.202	-.684**
	[.186]	[.137]	[.281]

Table 4
Robustness

This table displays equal- and value-weighted alphas by cybersecurity exposure portfolios under alternative expected return models and exposure definitions. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Returns are calculated as cum-dividend monthly returns. Rows 1-2 display CAPM alphas (Sharpe (1964)), rows 3-4 display Fama-French three-factor alphas (Fama and French (1993)), and rows 5-6 display Carhart four-factor alphas (Carhart (1997)). Rows 7-8 display five-factor alphas (Fama and French (2015)). In rows 1-6, stocks are sorted into High (Low) Exposure portfolios if their cybersecurity exposures are above (below) median in a given month. In rows 7-8, stocks are sorted into *High (Low) Exposure* portfolios if their six month rolling average cybersecurity exposures are above median. Portfolio returns are tracked over the following month, and portfolios are rebalanced on a monthly basis. A Long-short portfolio is formed in column (3) by going long on the *High Exposure* portfolio (column (2)) and shorting the *Low Exposure* portfolio (column (1)). Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Low Exposures	High Exposures	Long-Short (H-L)
	(1)	(2)	(3)
CAPM Alpha			
Equal-Weighted	.030	-.274	-.304*
	[.357]	[.261]	[.170]
Value-Weighted	.943***	.211	-.732***
	[.198]	[.160]	[.255]
3-Factor Alpha			
Equal-Weighted	.260	-.111	-.372**
	[.162]	[.123]	[.163]
Value-Weighted	.946***	.253*	-.693***
	[.172]	[.143]	[.262]
4-Factor Alpha			
Equal-Weighted	.262*	-.074	-.336**
	[.153]	[.116]	[.144]
Value-Weighted	.899***	.280**	-.619***
	[.153]	[.137]	[.233]
6mo Rolling Average Exposures			
Equal-Weighted	.143	-.155	-.298**
	[.156]	[.120]	[.144]
Value-Weighted	.775***	.290**	-.485*
	[.194]	[.130]	[.280]

Table 5
Double-Sorted Portfolios

This table displays equal- (column 1) and value-weighted (column 2) five-factor alphas (Fama and French (2015)) by cybersecurity exposure and Size (rows 1-2) and Book-to-Market ratios (3-4). The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Returns are calculated as cum-dividend monthly returns. Figures reflect five-factor alphas from long-short exposure portfolios formed in subsamples of below and above median Size (rows 1-2) and Book-to-Market ratio (3-4) stocks. Long-short exposure portfolios are formed by going long on the *High Exposure* portfolio and shorting the *Low Exposure* portfolio, where stocks are sorted into *High (Low) Exposure* portfolios if their cybersecurity exposures are above (below) median in a given month. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as heteroskedasticity-robust standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Equal-Weighted	Value-Weighted
	(1)	(2)
Size		
Low	-.532**	-.744*
	[.242]	[.391]
High	-.309**	-.676**
	[.131]	[.292]
B/M		
Low	-.492	-.909**
	[.323]	[.362]
High	-.382**	-.282
	[.147]	[.202]

Table 6
Fama-MacBeth Regressions

This table displays estimates from cross-sectional Fama-MacBeth regressions of returns on cybersecurity exposures. The dependent variable is the subsequent month's excess stock return, and regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The coefficients are reported as time-series averages of the estimates from the cross-sectional regressions. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Excess Return$_{t+1}$			
	(1)	(2)	(3)	(4)
High Exposures	-.326**	-.422***	-.369***	-.292***
	[.154]	[.131]	[.110]	[.109]
Beta		.472**	.323	.293
		[.216]	[.228]	[.229]
Size		.353**	.445***	.372***
		[.165]	[.151]	[.115]
B/M		-.523**	-.477**	-.325
		[.222]	[.224]	[.222]
Momentum			.593	.292
			[.430]	[.448]
Reversal			.192	.175
			[.236]	[.223]
Idiosyncratic Volatility			.602	.645
			[.546]	[.547]
Illiquidity			-.049	-.065
			[.073]	[.067]
CoSkew			.037	.072
			[.433]	[.443]
Max Stock Price			-.141	-.154*
			[.085]	[.083]
ROA				.506***
				[.083]
Asset Growth				.074
				[.137]
R&D Intensity				-.176
				[.107]
Observations	28286	28231	28120	28115
R-squared	.00	.10	.18	.20

Table 7
Cybersecurity Exposures and Extreme Negative Returns

This table displays regressions of extreme negative return incidences on cybersecurity exposures. The dependent variable is *3-σ Negative Return*, an indicator variable taking the value one if a firm experiences a return that is lower than three standard deviations below mean in the subsequent month, where standard deviation and mean are calculated over a lagging 60 month basis. Regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Industry is defined at the 2-digit NAICS level. Continuous regressors are normalized to have mean zero and standard deviation one. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and clustered at the firm level. (*** p<0.01, ** p<0.05, * p<0.10)

	3-σ Negative Return$_{t+1}$		
	(1)	(2)	(3)
ln(Cybersecurity Exposures)	.001*	.002**	.002**
	[.001]	[.001]	[.001]
Beta		-.012***	-.011***
		[.002]	[.002]
Size		-.016***	-.014***
		[.004]	[.004]
B/M		.001***	.002***
		[.001]	[.001]
Momentum		.000	.000
		[.001]	[.001]
Reversal		.000	.000
		[.000]	[.000]
Idiosyncratic Volatility		-.000	-.001
		[.001]	[.001]
Illiquidity		.000***	.000***
		[.000]	[.000]
CoSkew		.001**	.001**
		[.001]	[.001]
Max Stock Price		.013***	.012***
		[.004]	[.004]
ROA			-.003***
			[.001]
Asset Growth			.000
			[.001]
R&D Intensity			.000
			[.001]
Firm FE	Yes	Yes	Yes
Ind-Month FE	Yes	Yes	Yes
Observations	28068	27921	27916
R-squared	.36	.36	.36

Table 8
Cybersecurity Exposures and Future Breaches

This table displays regressions of future cybersecurity breaches on cybersecurity exposures. The dependent variable is an indicator variable taking the value one if a firm experiences a cybersecurity breach in the subsequent quarter. Regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The sample is further restricted to firms with data on cybersecurity breaches, where our breach data sample ends in 2021. Industry is defined at the 2-digit NAICS level. Continuous regressors are normalized to have mean zero and standard deviation one. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and clustered at the firm level. (*** p<0.01, ** p<0.05, * p<0.10)

	$\text{Breach}_{[t+1,t+3]}$		
	(1)	(2)	(3)
ln(Cybersecurity Exposures)	.007**	.007**	.007**
	[.003]	[.003]	[.003]
Beta		-.002	-.002
		[.003]	[.003]
Size		-.009	-.010
		[.008]	[.008]
B/M		.000	.000
		[.001]	[.001]
Momentum		-.000	-.000
		[.001]	[.001]
Reversal		.000	.000
		[.000]	[.000]
Idiosyncratic Volatility		.001	.001
		[.001]	[.001]
Illiquidity		.000	.000
		[.000]	[.000]
CoSkew		.002	.002
		[.002]	[.002]
Max Stock Price		.015*	.015*
		[.009]	[.009]
ROA			.001
			[.001]
Asset Growth			.001
			[.001]
R&D Intensity			-.001
			[.001]
Firm FE	Yes	Yes	Yes
Ind-Month FE	Yes	Yes	Yes
Observations	18388	18259	18255
R-squared	.24	.24	.24

Table 9
Cybersecurity Exposures and Future Profitability

This table displays regressions of profitability on cybersecurity exposures. The dependent variable is *Profitability*, which is defined as EBITDA divided by assets. Regressions are conducted at the firm-quarter level. The independent variable of interest is *ln(Average Cybersecurity Exposures)*, which is the logarithm of *Cybersecurity Exposures* averaged over a quarter. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Industry is defined at the 2-digit NAICS level. Continuous regressors are normalized to have mean zero and standard deviation one. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and clustered at the firm level. (*** p<0.01, ** p<0.05, * p<0.10)

	Profitability$_{t+1}$		
	(1)	(2)	(3)
ln(Avg. Cybersecurity Exposures)	-.001*	-.001*	-.001**
	[.001]	[.001]	[.000]
Size		.029***	.017***
		[.009]	[.005]
Asset Growth		14.835	17.341
		[12.450]	[12.035]
R&D Intensity		.434**	.412***
		[.181]	[.140]
B/M		-116.379	-63.892
		[236.399]	[230.806]
Leverage		-2.385**	-.347
		[1.037]	[.851]
Profitability			22.256***
			[3.917]
Firm FE	Yes	Yes	Yes
Ind-Quarter FE	Yes	Yes	Yes
Observations	6814	6592	6571
R-squared	.65	.67	.73

Table 10
Double-Sorted Portfolios by Investor Sophistication

This table displays equal- (column 1) and value-weighted (column 2) five-factor alphas (Fama and French (2015)) by cybersecurity exposure and investor sophistication. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Firm returns are calculated as cum-dividend monthly returns. Figures reflect five-factor alphas from long-short exposure portfolios formed in subsamples of stocks with below and above median *Investor Sophistication*, which is defined by fraction of stockholders who are non-passive. Long-short exposure portfolios are formed by going long on the *High Exposure* portfolio and shorting the *Low Exposure* portfolio, where stocks are sorted into *High (Low) Exposure* portfolios if their cybersecurity exposures are above (below) median in a given month. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Equal-Weighted	Value-Weighted
	(1)	(2)
Investor Sophistication		
Low	-.569*	-.808**
	[.307]	[.367]
High	-.140	-.235
	[.136]	[.196]

Table 11
Double-Sorted Portfolios by Cybersecurity Labor Tightness

This table displays equal- (column 1) and value-weighted (column 2) five-factor alphas (Fama and French (2015)) by cybersecurity exposure and cybersecurity labor market tightness. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Firm returns are calculated as cum-dividend monthly returns. Figures reflect five-factor alphas from long-short exposure portfolios formed in subsamples of stocks with below and above median *Cybersecurity Labor Tightness*, which is defined as the growth in wages for information security professionals (SOC code 151212) in a firm's headquarters state, after controlling for age, education, sex, and race. Long-short exposure portfolios are formed by going long on the *High Exposure* portfolio and shorting the *Low Exposure* portfolio, where stocks are sorted into *High (Low) Exposure* portfolios if their cybersecurity exposures are above (below) median in a given month. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Equal-Weighted	Value-Weighted
	(1)	(2)
Cybersecurity Labor Tightness		
Low	-.151	-.316
	[.145]	[.289]
High	-.758**	-1.277**
	[.351]	[.515]

Table 12
Double-Sorted Portfolios by Cybersecurity Attention

This table displays equal- (column 1) and value-weighted (column 2) five-factor alphas (Fama and French (2015)) by cybersecurity exposure and cybersecurity attention. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Firm returns are calculated as cum-dividend monthly returns. Figures reflect five-factor alphas from long-short exposure portfolios formed in subsamples of stocks with *High* and *Low Cybersecurity Attention*. *High Cybersecurity Attention* stocks are defined as having experienced a cybersecurity breach in the prior five years, while *Low Cybersecurity Attention* stocks are those that did not experience any breaches in the prior five years. Long-short exposure portfolios are formed by going long on the *High Exposure* portfolio and shorting the *Low Exposure* portfolio, where stocks are sorted into *High (Low) Exposure* portfolios if their cybersecurity exposures are above (below) median in a given month. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Equal-Weighted	Value-Weighted
	(1)	(2)
Cybersecurity Attention		
Low	-.422**	-.742**
	[.168]	[.289]
High	-.070	-.023
	[.317]	[.282]

Appendix

Variable Definitions

Asset Growth	Growth rate in total assets on an annual basis. Source: Compustat
Average Cybersecurity Exposures	*Cybersecurity Exposures* averaged over a quarter. Source: Rapid7
Beta	Market beta estimated over a trailing 60 month window. Source: CRSP
B/M	Ratio of book value of equity to market value of equity. Source: Compustat, CRSP
Breach	Indicator variable taking the value one if a firm experienced a cybersecurity breach, and zero otherwise. Source: Privacy Rights Clearinghouse
CoSkew	The coefficient estimate of the squared market excess return term, derived from a regression of monthly excess returns on market excess returns and squared market excess returns. Source: CRSP
Cybersecurity Exposures	Number of cybersecurity exposures for a firm in a given month. A cybersecurity exposure is defined as the number of Telnet (port number 23), Server Message Block (port numbers 139 and 445), Secure Shell (port number 22), and Remote Desktop Protocol (port number 3389) ports exposed to the public internet for IP addresses affiliated with the firm. Source: Rapid7
Cybersecurity Labor Tightness	Growth in residual salary for cybersecurity professionals in the firm's headquarter state. A cybersecurity professional is defined as an individual with SOC code = 151212. Residual salary is defined as the residuals derived from a regression of salary on age, education, sex, and race. Source: American Community Survey, Compustat
Excess Return	Monthly stock return minus the risk-free rate. Source: CRSP, Kenneth R French Data Library
High Exposures	Indicator variable taking the value one if a firm has above median Cybersecurity Exposures, and zero otherwise. Source: Rapid7
High Cybersecurity Labor Tightness	Indicator variable taking the value one if a firm has above median Cybersecurity Labor Tightness, and zero otherwise. Source: American Community Survey, Compustat
Idiosyncratic Volatility	The standard deviation of the residual series derived from a regression of monthly returns on the Fama-French three-factor model over a trailing 60 month window. Source: CRSP
Illiquidity	The ratio of daily absolute stock return to dollar trading volume, averaged within the month. Source: CRSP
Investor Sophistication	Fraction of shareholders that are non-passive, defined as not belonging to an index fund. Source: CRSP
Leverage	Total debt divided by total assets. Source: Compustat
Low Cybersecurity Attention	Indicator variable taking the value one if a firm has not experienced a reported cybersecurity breach over the past five years, and zero otherwise. Source: Privacy Rights Clearinghouse
Low Investor Sophistication	Indicator variable taking the value one if a firm has below median Investor Sophistication, and zero otherwise. Source: CRSP
Momentum	Cumulative stock return over an 11 month period from months t-12 to t-1. Source: CRSP
Profitability	EBITDA divided by total assets. Source: Compustat
R&D Intensity	R&D expense divided by total assets. Firms without reported R&D are assumed to have zero R&D. Source: Compustat
Reversal	Stock return over the one month period from months t-1 to t. Source: CRSP
ROA	Net income divided by total assets. Source: Compustat
Size	Market value of equity. Source: CRSP

Internet Appendix

Figure IA1

Cybersecurity Risk by Industry (Florackis et al., 2023)

This figure displays median cybersecurity risk by industry, as measured by Florackis et al. (2023). The sample reflects the sample from Florackis et al. (2023). Industry is defined by 2-digit NAICS codes, where 2-digit NAICS codes are displayed in parentheses beside the industry name. Detailed variable descriptions can be found in the Appendix.

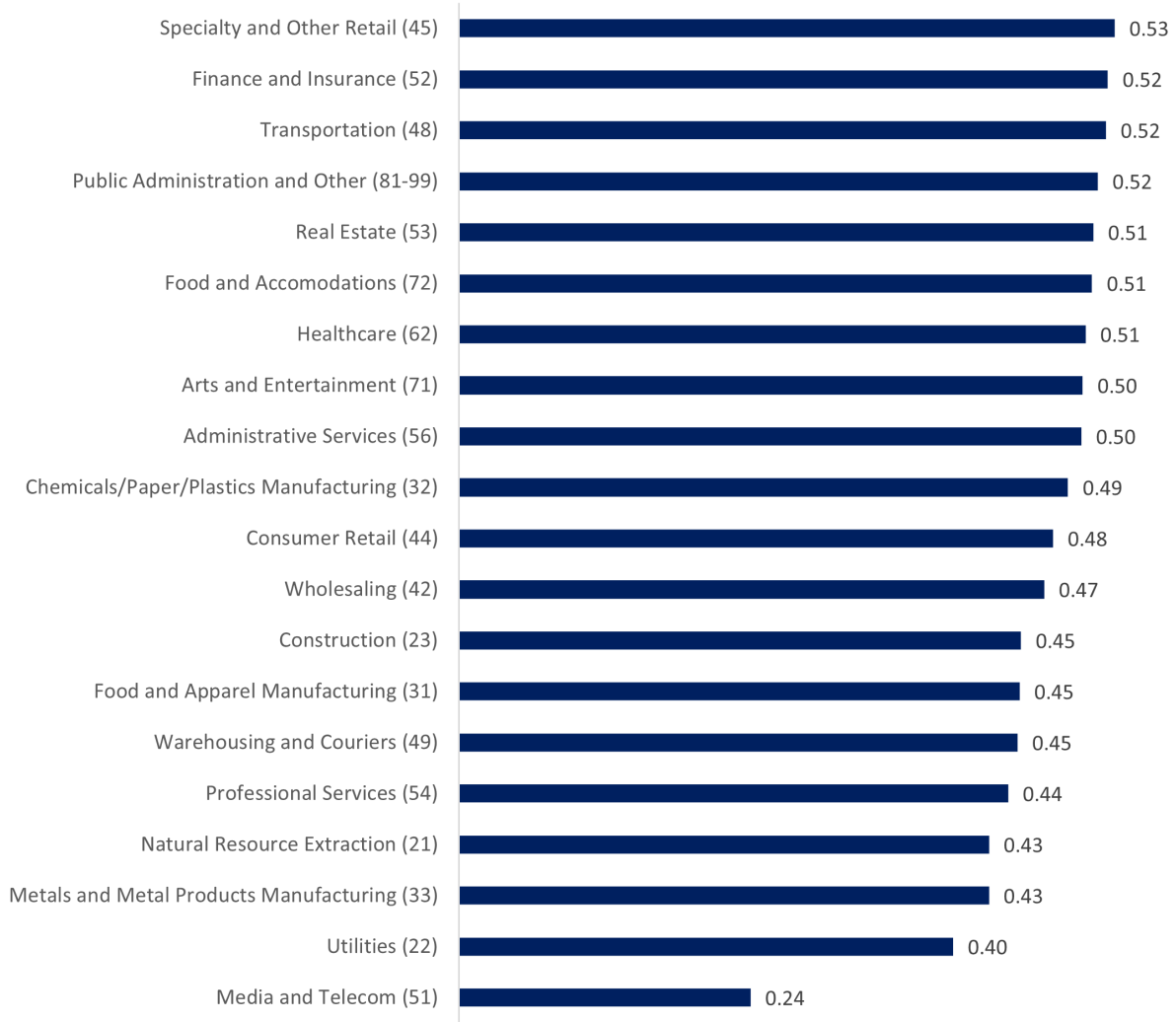

Figure IA2

Exposures versus Cybersecurity Labor Tightness

This figure displays a binscatter plot of logged *Cybersecurity Exposures* and *Cybersecurity Labor Tightness*. A regression of *ln(Cybersecurity Exposures)* on *Cybersecurity Labor Tightness* yields an estimated coefficient on *Cybersecurity Labor Tightness* of 0.12, significant at the 10% level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat.

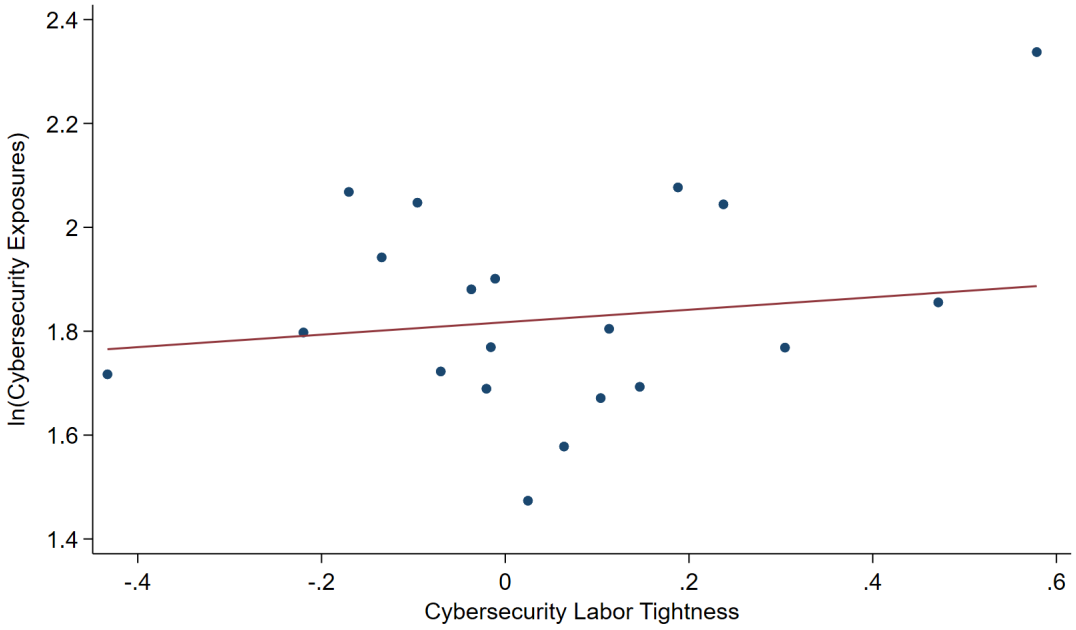

Figure IA3

Information Security Labor Market and Breaches

This figure displays the probability of a cybersecurity breach within one month (Panel A) and one quarter (Panel B) by *Cybersecurity Exposure* and *Cybersecurity Labor Tightness*. *High (Low) Exposure* is defined as firms with above (below) median *Cybersecurity Exposures*. *High (Low) Cybersecurity Labor Tightness* is defined as firms with above (below) median *Cybersecurity Labor Tightness*. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The sample is further restricted to firms with data on cybersecurity breaches, where our breach data sample ends in 2021.

Panel A: Breach Probability within One Month

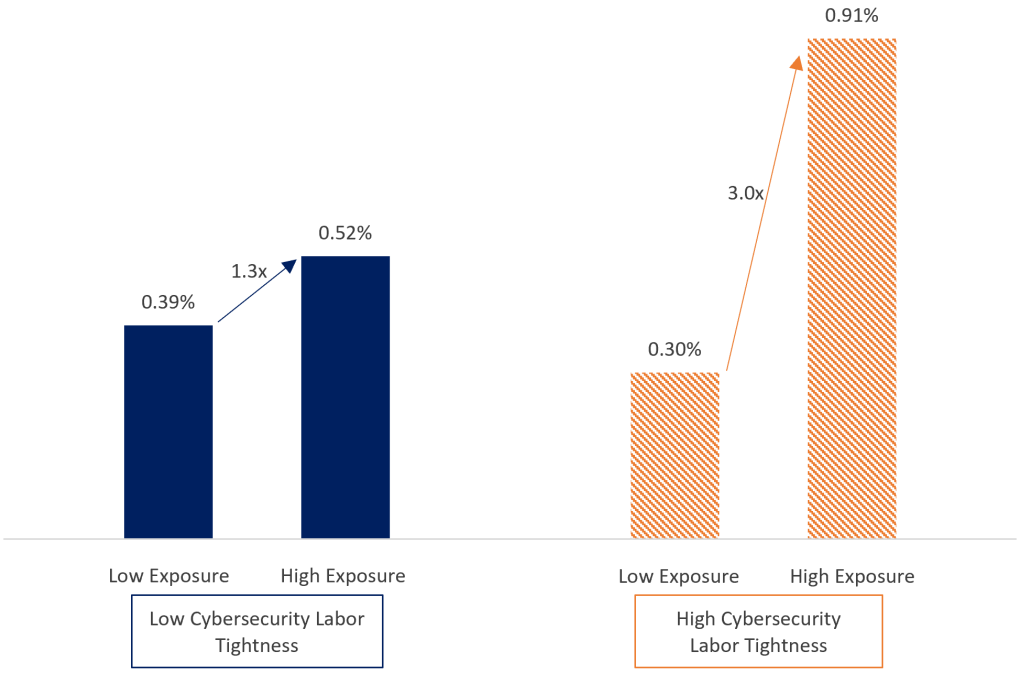

Figure IA3 (Continued)

Information Security Labor Market and Breaches

Panel B: Breach Probability within Three Months

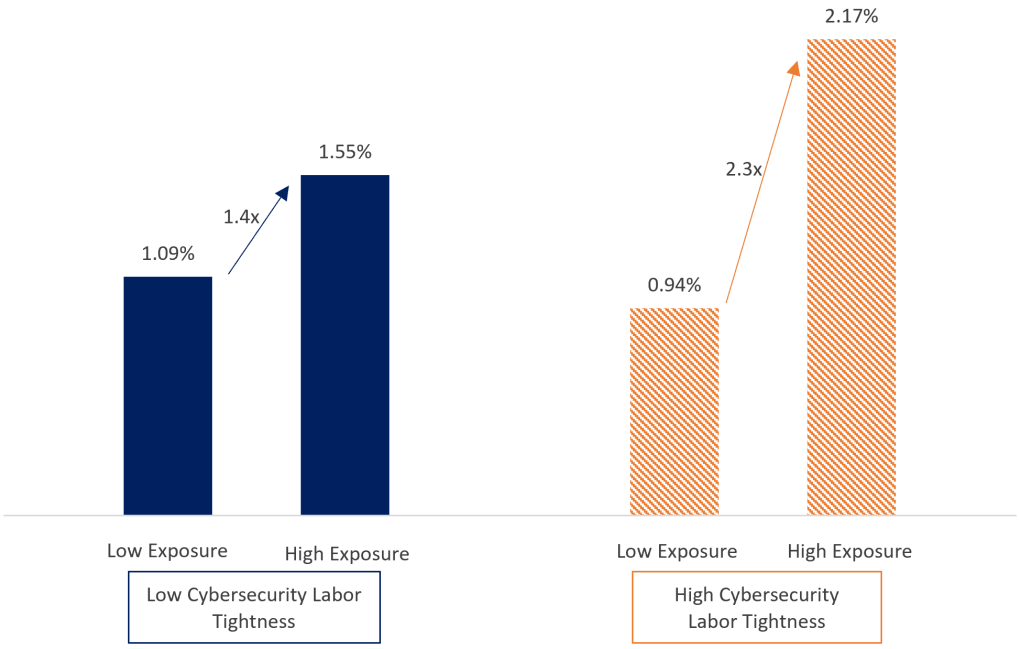

Figure IA4

Exposures by Cybersecurity Attention

This figure displays average cybersecurity exposures by cybersecurity attention. *High Cybersecurity Attention* is defined to be an indicator taking the value one if a firm experienced a cybersecurity breach over the past five years, and zero otherwise. Under a t-test, the difference in exposures across the two groups is significant at the 1% level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The sample is further restricted to firms with data on cybersecurity breaches, where our breach data sample ends in 2021.

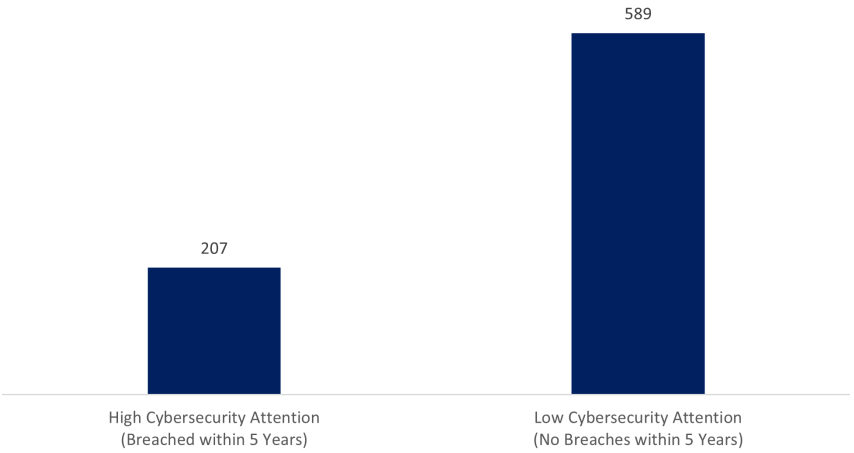

Figure IA5

Information Security Officers on Boards by Cybersecurity Attention

This figure displays the share of firms with an information security officer on the board by cybersecurity attention. A firm is identified as having an information security officer on its board if a director's role name contains the string "Information Security." Under a t-test, the difference in information security officer representation across the two groups is significant at the 1% level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The sample is further restricted to firms with data on cybersecurity breaches, where our breach data sample ends in 2021.

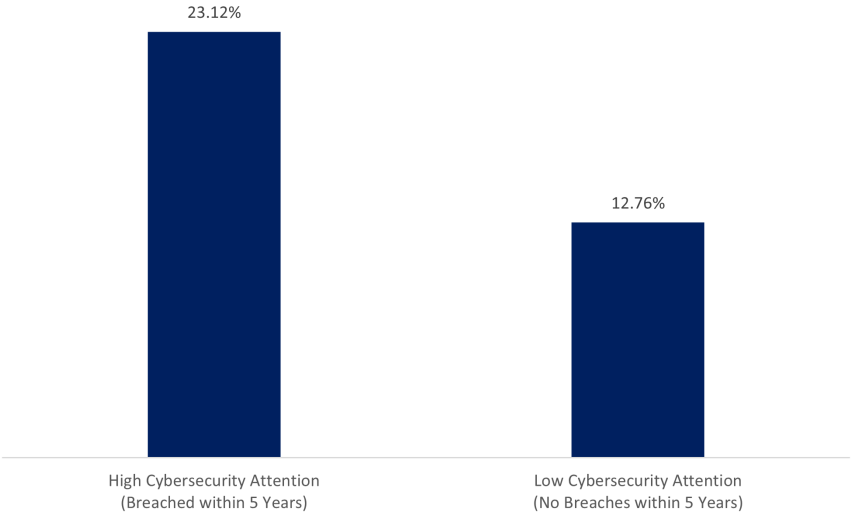

Table IA1
Descriptive Statistics for High Exposure Firms

This table displays descriptive statistics of key variables. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Detailed variable descriptions can be found in the Appendix.

	Percentile		
	25th	50th	75th
Cybersecurity Exposures	8.000	16.000	38.000
Excess Return (%)	-4.898	0.676	6.132
Size (Market Cap, USD mm)	10789.007	30217.672	80444.000
B/M	0.153	0.332	0.646
Profitability	0.017	0.027	0.040
ROA	0.004	0.011	0.022
Asset Growth	-0.012	0.007	0.029
R&D Intensity	0.000	0.000	0.002
Leverage	0.222	0.345	0.454
Beta	0.798	1.076	1.388
Momentum	0.912	1.086	1.276
Reversal	-4.898	0.676	6.132
Idiosyncratic Volatility	0.044	0.054	0.073
Illiquidity	-0.001	0.000	0.001
CoSkew	-0.027	0.003	0.037
Max Stock Price	47.226	88.473	157.282
Investor Sophistication	0.425	0.511	0.595
Cybersecurity Labor Tightness	-0.069	0.016	0.141

Table IA2
Descriptive Statistics for Low Exposure Firms

This table displays descriptive statistics of key variables. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Detailed variable descriptions can be found in the Appendix.

	Percentile		
	25th	50th	75th
Cybersecurity Exposures	0.000	0.000	3.000
Excess Return (%)	-4.955	0.825	6.328
Size (Market Cap, USD mm)	8260.098	18824.828	42736.746
B/M	0.177	0.412	0.669
Profitability	0.018	0.028	0.042
ROA	0.004	0.012	0.023
Asset Growth	-0.010	0.008	0.029
R&D Intensity	0.000	0.000	0.000
Leverage	0.226	0.354	0.462
Beta	0.746	1.118	1.457
Momentum	0.911	1.086	1.286
Reversal	-4.955	0.825	6.328
Idiosyncratic Volatility	0.046	0.058	0.077
Illiquidity	-0.001	0.000	0.002
CoSkew	-0.033	0.001	0.039
Max Stock Price	43.288	77.350	145.530
Investor Sophistication	0.409	0.490	0.572
Cybersecurity Labor Tightness	-0.069	0.016	0.139

Table IA3
Fama-MacBeth Regressions over Time

This table displays estimates from cross-sectional Fama-Macbeth regressions of returns on cybersecurity exposures. The dependent variable is the subsequent month's stock return, and regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The sample is further restricted to years 2018-2019 in column 1, 2020-2021 in column 2, and 2022-2024 in column 3. The coefficients are reported as time-series averages of the estimates from the cross-sectional regressions. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Return		
	2018-2019	2020-2021	2022-2024
	(1)	(2)	(3)
High Exposures	-.143	-.471**	-.268
	[.101]	[.177]	[.196]
Beta	-.294	.474	.548
	[.226]	[.409]	[.337]
Size	.462***	.527*	.212
	[.138]	[.288]	[.138]
B/M	-.398	-.397	-.229
	[.547]	[.404]	[.322]
Momentum	-1.089	1.118	.624
	[.838]	[.736]	[.569]
Reversal	-.269	.886**	-.015
	[.296]	[.392]	[.296]
Idiosyncratic Volatility	-.059	2.584*	-.198
	[.494]	[1.275]	[.211]
Illiquidity	-.014	-.166	-.029
	[.125]	[.142]	[.079]
CoSkew	.173	.324	-.161
	[.163]	[1.449]	[.305]
Max Stock Price	-.109**	-.278	-.098*
	[.036]	[.261]	[.054]
ROA	.644***	.611***	.349***
	[.094]	[.183]	[.116]
Asset Growth	.114	-.296	.296**
	[.088]	[.346]	[.136]
R&D Intensity	-.179**	-.234	-.135
	[.067]	[.286]	[.146]
Observations	9005	8882	10228
R-squared	.17	.21	.21

Table IA4
Fama-MacBeth Regressions (with Industry Fixed Effects)

This table displays estimates from cross-sectional Fama-Macbeth regressions of returns on cybersecurity exposures, controlling for industry fixed effects. Industry is defined at the 2-digit NAICS level. The dependent variable is the subsequent month's stock return, and regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The coefficients are reported as time-series averages of the estimates from the cross-sectional regressions. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Return
	(1)
High Exposures	-.275***
	[.092]
Beta	.272
	[.236]
Size	.343**
	[.129]
B/M	-.546**
	[.233]
Momentum	.141
	[.450]
Reversal	.275
	[.278]
Idiosyncratic Volatility	.712
	[.513]
Illiquidity	-.116
	[.103]
CoSkew	.175
	[.554]
Max Stock Price	-.189
	[.130]
ROA	.538***
	[.088]
Asset Growth	.019
	[.135]
R&D Intensity	-.079
	[.104]
Industry FEs	Yes
Observations	28096
R-squared	.30

Table IA5
Fama-MacBeth Regressions (Horserace)

This table displays estimates from cross-sectional Fama-Macbeth regressions of returns on cybersecurity exposures. The dependent variable is the subsequent month's stock return, and regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. *Cybersecurity Risk (Florackis et al. (2023))* is Florackis et al. (2023)'s text-based cybersecurity risk, measured in 2017. *Cybersecurity Risk (Florackis et al. (2023))* is measured in 2017 since 2017 is the last year of the Florackis et al. (2023) sample. The coefficients are reported as time-series averages of the estimates from the cross-sectional regressions. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Return
	(1)
High Exposures	-.315***
	[.108]
Cybersecurity Risk (Florackis et al. (2023))	.084
	[.070]
Beta	.309
	[.238]
Size	.375***
	[.122]
B/M	-.343
	[.224]
Momentum	.385
	[.448]
Reversal	.166
	[.241]
Idiosyncratic Volatility	.631
	[.560]
Illiquidity	-.100
	[.069]
CoSkew	.070
	[.489]
Max Stock Price	-.146*
	[.083]
ROA	.493***
	[.096]
Asset Growth	.109
	[.135]
R&D Intensity	-.162
	[.112]
Observations	26398
R-squared	.21

Table IA6
Cybersecurity Exposures and Extreme Positive Returns

This table displays regressions of extreme positive return incidences on cybersecurity exposures. The dependent variable is *3-σ Positive Return*, an indicator variable taking the value one if a firm experiences a return that is greater than three standard deviations above mean in the subsequent month, where standard deviation and mean are calculated over a lagging 60 month basis. Regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. Industry is defined at the 2-digit NAICS level. Continuous regressors are normalized to have mean zero and standard deviation one. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and clustered at the firm level. (*** p<0.01, ** p<0.05, * p<0.10)

	3-σ Positive Return$_{t+1}$		
	(1)	(2)	(3)
ln(Cybersecurity Exposures)	-.000	-.000	-.000
	[.001]	[.001]	[.001]
Beta		-.006***	-.006***
		[.001]	[.001]
Size		-.013***	-.013***
		[.003]	[.003]
B/M		.001**	.001**
		[.000]	[.000]
Momentum		-.001	-.001
		[.001]	[.001]
Reversal		-.001	-.001
		[.001]	[.001]
Idiosyncratic Volatility		-.003***	-.003***
		[.000]	[.000]
Illiquidity		-.000**	-.000**
		[.000]	[.000]
CoSkew		-.002**	-.002**
		[.001]	[.001]
Max Stock Price		.004*	.004*
		[.002]	[.002]
ROA			-.000
			[.001]
Asset Growth			.000
			[.001]
R&D Intensity			-.001
			[.001]
Firm FE	Yes	Yes	Yes
Ind-Month FE	Yes	Yes	Yes
Observations	28068	27921	27916
R-squared	.15	.16	.16

Table IA7
Investor Sophistication and the Cross Section of Returns

This table displays estimates from cross-sectional Fama-MacBeth regressions of returns on cybersecurity exposures and investor sophistication. The dependent variable is the subsequent month's excess stock return, and regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The coefficients are reported as time-series averages of the estimates from the cross-sectional regressions. *Low Investor Sophistication* stocks are those with below median *Investor Sophistication*, which is defined by fraction of stockholders who are non-passive. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Excess Return$_{t+1}$			
	(1)	(2)	(3)	(4)
High Exposures × Low Investor Sophistication	-.346	-.587*	-.446**	-.382**
	[.351]	[.299]	[.210]	[.189]
High Exposures	-.125	-.088	-.121	-.067
	[.169]	[.150]	[.136]	[.137]
Low Investor Sophistication	.198	.034	-.130	-.197
	[.283]	[.383]	[.203]	[.186]
Beta		.474**	.349	.313
		[.219]	[.229]	[.228]
Size		.432**	.535***	.460***
		[.185]	[.148]	[.113]
B/M		-.552**	-.511**	-.353
		[.224]	[.216]	[.213]
Momentum			.476	.142
			[.424]	[.436]
Reversal			.212	.167
			[.246]	[.227]
Idiosyncratic Volatility			.660	.751
			[.564]	[.579]
Illiquidity			-.082	-.091
			[.074]	[.067]
CoSkew			.152	.198
			[.520]	[.533]
Max Stock Price			-.144*	-.153*
			[.083]	[.080]
ROA				.575***
				[.099]
Asset Growth				.082
				[.136]
R&D Intensity				-.196*
				[.106]
Observations	28089	28036	27926	27921
R-squared	.01	.11	.19	.21

Table IA8
Cybersecurity Labor Tightness and the Cross-Section of Returns

This table displays estimates from cross-sectional Fama-MacBeth regressions of returns on cybersecurity exposures and cybersecurity labor market tightness. The dependent variable is the subsequent month's excess stock return, and regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The coefficients are reported as time-series averages of the estimates from the cross-sectional regressions. *High Cybersecurity Labor Tightness* stocks are those with above median *Cybersecurity Labor Tightness*, which is defined as the growth in wages for information security professionals (SOC code 151212) in a firm's headquarters state, after controlling for age, education, sex, and race. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Excess Return$_{t+1}$			
	(1)	(2)	(3)	(4)
High Exposures × High Cybersecurity Labor Tightness	-.658**	-.546*	-.405*	-.381*
	[.310]	[.281]	[.204]	[.219]
High Exposures	-.186	-.339**	-.341**	-.261*
	[.173]	[.156]	[.139]	[.142]
High Cybersecurity Labor Tightness	.492	.378	.389*	.411
	[.332]	[.268]	[.219]	[.251]
Beta		.641**	.461*	.430
		[.247]	[.273]	[.273]
Size		.361	.499**	.416***
		[.229]	[.202]	[.150]
B/M		-.497**	-.398*	-.262
		[.222]	[.201]	[.192]
Momentum			.678	.359
			[.483]	[.516]
Reversal			.380	.335
			[.283]	[.270]
Idiosyncratic Volatility			.848	.889
			[.742]	[.750]
Illiquidity			-.112	-.113
			[.078]	[.077]
CoSkew			.198	.245
			[.578]	[.591]
Max Stock Price			-.134	-.146
			[.108]	[.102]
ROA				.530***
				[.106]
Asset Growth				.054
				[.202]
R&D Intensity				-.180
				[.151]
Observations	20506	20468	20403	20401
R-squared	.01	.12	.20	.22

Table IA9
Cybersecurity Attention and the Cross Section of Returns

This table displays estimates from cross-sectional Fama-MacBeth regressions of returns on cybersecurity exposures and cybersecurity attention. The dependent variable is the subsequent month's excess stock return, and regressions are conducted at the stock-month level. The sample reflects Fortune 500 firms from 2018 through December 2024 with available cybersecurity exposure data that can be matched to CRSP and Compustat. The coefficients are reported as time-series averages of the estimates from the cross-sectional regressions. *Low Cybersecurity Attention* stocks are those that did not experience any breaches in the prior five years. Detailed variable descriptions can be found in the Appendix. Standard errors are reported in brackets and calculated as Newey-West standard errors. (*** p<0.01, ** p<0.05, * p<0.10)

	Excess Return$_{t+1}$			
	(1)	(2)	(3)	(4)
High Exposures × Low Cybersecurity Attention	-.388*	-.464**	-.378**	-.394**
	[.206]	[.196]	[.174]	[.180]
High Exposures	.022	-.004	-.019	.068
	[.186]	[.137]	[.156]	[.160]
Low Cybersecurity Attention	.442	.508*	.604**	.518*
	[.282]	[.273]	[.263]	[.284]
Beta		.477**	.329	.300
		[.216]	[.228]	[.228]
Size		.360**	.453***	.383***
		[.166]	[.151]	[.114]
B/M		-.513**	-.465**	-.311
		[.219]	[.223]	[.222]
Momentum			.604	.310
			[.427]	[.444]
Reversal			.194	.173
			[.238]	[.225]
Idiosyncratic Volatility			.601	.645
			[.547]	[.550]
Illiquidity			-.049	-.064
			[.072]	[.066]
CoSkew			.032	.064
			[.433]	[.443]
Max Stock Price			-.140	-.152*
			[.085]	[.083]
ROA				.500***
				[.083]
Asset Growth				.072
				[.138]
R&D Intensity				-.177
				[.111]
Observations	28286	28231	28120	28115
R-squared	.01	.11	.18	.20