JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2025, tyaf032
https://doi.org/10.1093/cybsec/tyaf032

Research paper

Are cybersecurity firms different? Intra-sector and cross-industry comparisons of financial performance

Loïc Maréchal [1,*], Alain Mermoud [2], Dimitri Percia David [1], Mathias Humbert [3]

[1]Institute of Entrepreneurship & Management, University of Applied Sciences, HES-SO Valais-Wallis - 3960, Sierre, Switzerland
[2]Cyber-Defence Campus—Armasuisse, Science and Technology - 1015, Lausanne, Switzerland
[3]Department of Information Systems, HEC Lausanne, University of Lausanne - 1015, Lausanne, Switzerland

*Corresponding author: Loïc Maréchal, Institute of Entrepreneurship & Management, University of Applied Sciences HES-SO Valais-Wallis, Le Foyer Techno-Pôle 1, 3960, Sierre, Switzerland. E-mail: loic.marechal@hevs.ch

Received 18 July 2023; revised 1 July 2025; accepted 23 September 2025

Abstract

Early-stage firms play a crucial role in driving innovation and developing new products and services, particularly in the field of cybersecurity. Therefore, evaluating their performance is vital for investors and policymakers. This work presents a financial evaluation of early-stage firms' performance in 19 cybersecurity sectors using a private-equity dataset from 2010 to 2022 retrieved from Crunchbase. We compare cybersecurity sectors regarding the amount raised over funding rounds and post-money valuations while inferring missing observations with a machine-learning method. We observe significant investor interest variations across categories, periods, and locations. In particular, we find the average capital raised (valuations) to range from USD 7.24 mln (USD 32.39 mln) for spam filtering to USD 45.46 mln (USD 447.22 mln) for the private cloud sector. We additionally find that the entire cybersecurity sector is both underfunded and undervalued with respect to the broader information technology sector. Next, we assume a log process for returns computed from post-money valuations and estimate the expected returns, systematic and specific risks, and risk-adjusted returns of investments in early-stage firms belonging to the cybersecurity sector. Again, we observe substantial performance variations with annualized expected returns ranging from 9.72% for privacy to 177.27% for the blockchain sector. Whereas expected returns on the cybersecurity sector are on par with those of other sectors, its systematic risk is lower, indicating a contra-cyclical nature. By estimating the performance of cybersecurity investments, we shed light on variations in market expectations across cybersecurity sectors and compared to other sectors.

Keywords: investment in information security; cybersecurity; asset pricing; machine learning; venture capital

Introduction

> If it were measured as a country, then cybercrime—which is predicted to inflict damages totaling 6 trillion USD globally in 2021—would be the world's third-largest economy after the U.S. and China (Cybersecurity Ventures, available at https://cybersecurityventures.com/hackerpocalypse-cybercrime).

In this 2020 article, "Cybersecurity Ventures" additionally expects the global costs of cyberattacks to increase by 15% per year over the next 5 years, reaching USD 10.5 trillion annually by 2025. This represents the most significant transfer of wealth in history, surpassing the trade of all illegal drugs combined. To mitigate these costs, the information security industry, particularly cybersecurity, is expected to experience significant growth. Indeed, these firms develop and implement new solutions to increase security in IT systems, protect virtual assets, custom sensitive information, or secure transactions and communications.

To better understand the maturity of the cybersecurity ecosystem and sustain its growth, it is critical to evaluate the financial performance of cybersecurity firms. First, their valuations and corresponding expected returns provide us with an almost direct metric for the potential of cybersecurity. It also helps disentangle the different cybersecurity sectors regarding capital raised and valuations, which this capital translates into, thus enhancing technology monitoring. Second, estimating financial performance parameters such as systematic financial risk and risk-adjusted returns helps guide investors' decisions. This will ultimately enable optimal capital allocation across target firms, thereby improving the sector's economic health and enhancing its ability to raise the global standard of cybersecurity.

In this research, we estimate the realized and expected financial performance of private firms involved in cybersecurity. We choose to estimate our parameters in private firms for three reasons. First, we can observe a larger cross-section of firms than for public equity. Second, the likelihood of cybersecurity firms having a single core business in the target sub-sector is significantly higher for small and medium-sized firms, which are typically privately owned. Lastly, cybersecurity businesses are generally smaller, and few firms are listed, which would further limit the number of observations. As anecdotal evidence, the S&P 500 does not include any component that is a pure cybersecurity company, even though four out of five top components are technology companies. We focus on the realized financial performance of 19 cybersecurity-related sectors identified in Crunchbase, a global database containing commercial and managerial data for private and public companies. In particular, we scrutinize their data about funding rounds, (post-money) firm valuations, and exits (IPOs or acquisitions). We restrict our sample to 2010–2022 for two reasons. First, Crunchbase is relatively recent, and many observations are missing before 2010. For instance, nearly 88% of the recorded funding rounds occurred after 2010. Second, the magnitude of cyberattacks and the importance of the cybersecurity industry have vastly increased since 2010. Crunchbase data are exhaustive regarding funding rounds. Still, many valuations and IPO share price observations are missing. We employ a machine learning approach to estimate them based on the numerous highly correlated variables in the dataset. We next follow Cochrane's (2005) approach to compute returns from financing rounds to "exits," i.e. IPOs or acquisitions [1]. While data incompleteness and heterogeneity are common concerns when working with Crunchbase, our empirical strategy explicitly addresses these limitations. The machine learning model we apply enables us to impute missing values, such as post-money valuations (PMVs) and IPO prices, using patterns in the extensive set of correlated firm-level variables available in the dataset. This helps reduce information loss and maintain robustness in estimation. Additionally, the use of Cochrane's (2005) maximum likelihood approach allows us to correct for potential selection bias that may arise from nonrandom observation of financing rounds and exits. Together, these techniques substantially enhance the credibility of our financial performance estimates, despite the inherent constraints of the dataset. We compute returns that account for capital dilution, as multiple funding rounds before exits are common in the venture capital (VC) business.

We first identify that the top three sectors based on the capital raised criterion are artificial intelligence, security, and machine learning, with more than USD 60 bln raised in each. Additionally, the private cloud sector dominates in terms of average and median funding and PMVs, with an average firm valuation of up to USD 45.46 million. We also find that artificial intelligence and machine learning dominate other sectors in total valuations. These sectors offer returns of up to USD 10 in share valuation for every USD invested. We repeat this exercise for the broader cybersecurity industry and other sectors, in particular information technology (IT), from which we exclude cybersecurity firms. We find, in particular, that both average funding and average PMVs are lower for the cybersecurity industry than it is for IT, with USD 19.04 mln (23.06) and USD 154.65 mln (165.83). Similarly, we find that the cybersecurity firms' time to exit, a measure of the sector's success, is significantly higher (almost 5 years) than for all other sectors, including IT (3.5 years).

We next assume a log return process and calculate returns to exit, accounting for capital dilution in 12 cybersecurity sectors. We find that α, return in excess of the market risk premium, is positive for all technologies, while β, standing for the systematic risk and cyclicality, ranges between 0.51 and 5.51. We find sectors such as artificial intelligence to be pro-cyclical, while firms in the more explicit cybersecurity sector have β below one, indicative of contra-cyclicality. Overall, we find the cybersecurity industry ($\beta = 1.62$) to be slightly less procyclical than the IT industry ($\beta = 1.81$). Finally, we compute the implied expected arithmetic and log returns from model parameters. We find the blockchain sector to have the highest expected arithmetic and log returns at 177.27% and 105.42%, respectively, consistent with the performance of cryptocurrencies over the sample period. Artificial intelligence is the second-highest sector, with expected annualized arithmetic returns of 67.25%, far higher. Other sectors with high expected returns include machine learning, private cloud, and cloud security, whereas the lowest ranks include privacy (9.72% p.a.) and biometrics (23.22% p.a.). On this aspect, the cybersecurity industry delivers an annualized expected seven points lower than for IT (37.43% vs 44.40%, but on par with the retail sector.

Our research sheds light on the significant performance variations across cybersecurity sectors, including funding, valuations, probability of success, cyclicality, and adjusted expected returns. It also sheds light on the undervaluation of cybersecurity firms with respect to other industries in general. In particular, with lower average funding and valuations, a longer time to exit, a larger number of investors, less procyclicality, and lower adjusted returns, the cybersecurity industry's performance significantly diverges from that of the IT sector, potentially offering new explanations for under-investment in the industry from potential investors and customers.

The remainder of this paper is organized as follows. The section "Literature review and contribution" presents a literature review relevant to our work, highlighting our contributions. The section "Data and methodology" details the data and methods, the section "Results" presents the results, and the section "Conclusion" concludes.

Literature review and contribution

Estimation challenges

Studies in VC markets face two problems. First, as opposed to public companies, private firms are not legally required to disclose their financial statements. For instance, in the US, this is done through the Securities and Exchange Commission. Additionally, private firms are not required to communicate with their shareholders through an annual report. Second, private firms have no publicly traded shares, and we do not observe any prices or market capitalizations. Thus, almost none of the public equity methods are readily usable. Yet, private firms issue shares to investors. Thus, the standard practice for VC analysts is to value a company around these financing events (a financing event is any event during which the firm receives equity, issues debt, or receives grants). This valuation is called pre- (post-)money valuation when done before (after) the event. An analyst obtains the firm's valuation by multiplying the per-share price of the most recent event by the fully diluted number of common shares. This calculation, however, does not account for the optionality of the investment contract and assumes that all shares have the same value, regardless of their type (common, preferred, or convertible notes). See, e.g. Gornall & Strebulaev [2].

Venture capital valuation

One method that allows estimating expected returns and systematic and idiosyncratic risks in VC is considering sectors and not individual firms, thereby leveraging more information. In particular, Cochrane (2005) uses a maximum likelihood estimation method to obtain these values [1]. He finds a mean arithmetic return of 59%, an alpha of 32%, a beta of 1.9, and a volatility of 86% (corresponding to a 4.7% daily volatility). He fits a logarithmic model because of the returns distribution, which is heavily positively skewed. Given that successful firms are likely to be over-represented in his sample, he directly includes a selection bias parameter in the likelihood function. Ewens (2009) updates the methodology, focusing on round-to-round returns [3]. He obtains an alpha of 27% and a beta of 2.4. He additionally finds that 60% of all investments have negative returns and high idiosyncratic volatility. Korteweg and Nagel (2016) use an alternative approach and estimate monthly arithmetic alphas of 3.5% for VC funds [4]. Conversely, Moskowitz et al. (2002) conclude that VC returns are not higher than public equity [5].

In a second strand of research, Alexon and Martinovic (2015) and Franzoni et al. (2012) estimate abnormal returns and risk factor loadings with standard regressions by using internal rates of return [6,7]. Driessen et al. (2012) and Ang et al. (2018) extend this approach to a dynamic setting in which they solve for abnormal returns and risk exposures using the generalized method of moments. This approach requires only a cross-section of observable investment cash flows [8,9].

The third line of research attempts to identify successful features of exits or features explaining venture valuations. Cumming and Dai (2011) identify a convex relationship between fund size and firm valuations and a concave one between fund size and a target company's performance [10]. Similarly, Cumming and Dai (2010) examine local bias in VC investments and relate geographical distance to the target firm valuation [11]. Engel and Keilbach (2007) find that VC-funded firms have more patent applications than those funded differently before investment, suggesting that venture capitalists focus on commercializing existing innovations [12].

The literature on the topic is sparse, and there is no consensus on methodology. Nonetheless, previous works estimate similar values. Cochrane's (2005) method stands out for its simplicity and has been successfully used in later research. It also focuses on returns from rounds to IPO, which is not the case for Korteweg and Sorensen (2010) [13]. Another strand of the literature concerns the construction of indices and benchmarks related to VC performance. See, e.g. Peng (2001), Hwang et al. (2005), Schmidt (2006), Cumming et al. (2013), and McKenzie et al. (2012) [14–18].

Financial performance of cybersecurity-providing firms

We are only aware of two studies that focus on the financial performance of the cybersecurity sector. First, Mezzetti et al. (2024) use a bipartite graph to link early-stage cybersecurity firms to technologies and rank them based on features such as the type of investors or geographic distance between investors and firms [19]. However, the ranking is relative and depends on investors' preferences. Second, Burguet et al. (2024) employ Cochrane's (2005) approach and update his results on a more recent period based on a more exhaustive dataset [1,20]. However, their primary focus is the broad financial performance of VC firms, not specifically cybersecurity. Moreover, they estimate the financial performance of the "security" sector that does not include all categories we consider representative. Most importantly, they do not assess the sub-sector performance. Based on these research gaps, our research questions are: How do cybersecurity firms perform financially? Is this performance homogeneous across information security sub-sectors? We bring several contributions to cybersecurity economics and the financial literature by answering these questions.

First, we bring new perspectives on the economics of cybersecurity by measuring the performance of providing firms and comparing it to other non-cyber sectors. Second, we refine this comparison by examining the heterogeneity of performance across cybersecurity sub-sectors. Third, since financial performance represents investors' expectations, our results implicitly forecast future developments in cyber risks and mitigation measures. Once again, we compare our cybersecurity estimates to those of other, more traditional sectors, particularly the broader information technology sector.

Data and methodology

Data

Crunchbase

Crunchbase is a global commercial, financial, and managerial data vendor for private and public companies. Created in 2007 by TechCrunch, it has been maintained by Crunchbase Inc. since 2015 [21]. This database is used by academics, NGOs, and industry practitioners [22,23]. Crunchbase collects data daily by combining crowdsourcing, NLP-based newswire analyses, and in-house processing. It also complements it with data from third-party providers. The dataset is organized into several entities, including those relevant to this study. First, "organizations" is the set reporting administrative information on private and public companies, funds, or institutions. It includes business information, contact details, location, number of employees, and sector of activity. Second, "people" contain information about individuals involved with a firm. It includes age, CV, degrees, or gender. Third, "funding rounds" includes funded companies, investors, round types (seed, series A/B/C,..., or debt issuing), and the amount of money raised. Fourth, "exits" reports the firm's acquisitions and their types (LBOs, management buyouts, or mergers) as well as IPO-related information (new listing or delistings, share prices, market capitalization, and exchange venue). Crunchbase includes additional business information that is irrelevant to our research and therefore not discussed in this context.

One caveat of the dataset is that many observations regarding funding rounds are missing. In particular, PMVs and IPO share prices, which are central to our study, are often unavailable. Moreover, the multiple sources of information for Crunchbase data may induce heterogeneity, and the quality of the observations will likely vary across countries, industries, or periods. For instance, US companies are over-represented compared to those of other nations. Finally, the observations were almost nonexistent before the 2000s and sparse before the 2010s. However, we assume that this latter issue will have only a mild impact on our study, as our goal is to estimate the current financial performance of cybersecurity sectors. Moreover, Crunchbase has a stronger focus on the technology industry, which is an advantage for this research. We address the issues of missing data and potential selection bias using two complementary approaches: a machine

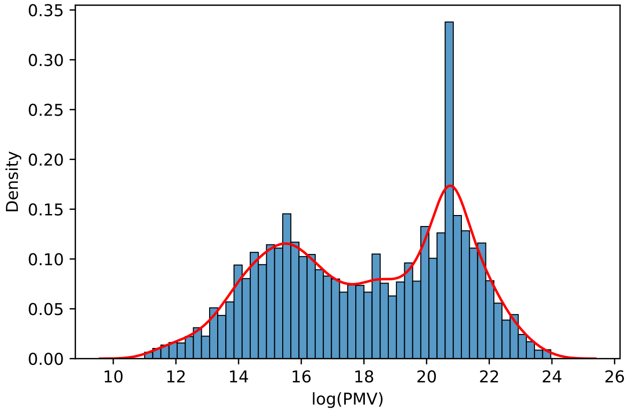

Figure 1. PMVs distributions from Crunchbase firms of all categories. This figure depicts the distribution of the logarithm of all PMVs of firms of all industries available in Crunchbase. The bars depict the discrete density; the red line is the kernel distribution. The period is 2010–2022.

Table 1. Features used for the inference with PMVs regression.

Symbol	Description
T	Date of the round (in days, relative to 1/1/1926)
ΔT	Number of days since the last financing event
M	Amount of money raised ($)
ΔM	Difference of money raised since the last round ($)
N	Number of investors for the current round
R	Lead investor rank for the current round
S	Industry sector (categorical)
G	Geographical position (categorical)

This Table lists the features selected from the Crunchbase dataset to model the missing observations of PMVs in certain funding rounds.

learning-based classification and imputation model, and the maximum likelihood estimation method developed by Cochrane (2005). These methods enable us to estimate financial performance metrics robustly, despite gaps in the data, and to correct for distortions introduced by non-random observation patterns. As such, while the limitations of Crunchbase are real, they do not invalidate our findings; rather, they are explicitly accounted for in our empirical strategy.

We download data until May 2022; nearly 88% of the recorded funding rounds occurred after 2010, and the trend is upward. This is due to the availability of data and the fact that the VC market has vastly increased since the 2008 global financial crisis. Our restricted cybersecurity-related sectors dataset, detailed below, comprises a total of 21,234 funding rounds. In the first column of Table 2, we report the number of funding rounds for each sub-sector. In Appendix, Table A1, we provide randomly selected examples of firms present in each Crunchbase sector from their classification. Although we cannot rule out the possibility of misclassification from other firms, the fact that none of the randomly selected companies are misclassified in any sector gives us confidence that the Crunchbase classification is relevant.

Market data

We fit the model on one public equity benchmark and one risk-free asset. We use two sources: Yahoo Finance and the Federal Reserve Bank of St. Louis (FRED) (Yahoo Finance, https://finance.yahoo.com/lookup/). From their APIs, we collect the returns on the S&P 500 index. For the risk-free asset, we use the 3-month T-Bill rate, which helps for our analysis since we use a time grid of 3 months to fit the model (Board of Governors of the Federal Reserve System (US), 3-Month Treasury Bill Secondary Market Rate, Discount Basis [TB3MS], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/TB3MS). Given the low frequency of observations, it is also the standard in the existing VC research.

Methodology

Missing data interpolation

To circumvent the problem of missing PMVs and, to a lesser extent, missing funding round amounts, we interpolate the missing data, leveraging the other features of the database using an ML regression approach. To leverage all the information in the database, we use the entire set, including firms that do not belong to the cybersecurity sub-sectors, to estimate the missing PMVs. We also attempt to train models for each sector. However, the smaller training set sizes did not allow the model to generalize, yielding errors too large at the validation step. We depict the data treatment process in the top panel of Appendix Fig. A1. We are not interested in the precise value of the firm after a financing event but rather in an unbiased estimate of the order of magnitude of the business value. We plot the distribution of the PMVs reported by Crunchbase for all firms in Fig. 1. Note that PMVs follow a bi-modal distribution, centered roughly around the 2–3 million value ($e^{15} \approx 3e6$) and the billion value ($e^{21} \approx 1e9$). This is likely due to the round number bias studied in e.g. Herve and Schwienbacher (2018). Financial analysts stick to round numbers because of the lack of firm information and the high valuation risks involved [24].

We report the features in Table 1 and capitalize on the high correlation between funding round size and PMVs and between funding round frequency and PMVs, respectively. Also see Alexy et al. (2012) [25]. The particular implementation used in this project is “AutoSklearn” [26].

Taxonomy and classification

Although taxonomies and classifications of cyber events are numerous, those for the corresponding cybersecurity technologies that mitigate these threats are not readily available (see, e.g. Agrafiotis et al. (2018) for a taxonomy of cyberattacks and Shameli et al. (2016) for a taxonomy of information security risk assessment (ISRA), and NIST [27–29]). Despite the more extensive availability of cyberattacks taxonomies, Ruan (2017) advocates for a more consistent taxonomy of cyber incidents [30]. To classify firms, we use Crunchbase tags that we select to resemble that of the ENISA cybersecurity market analysis framework (see, https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf and of Hwang et al. (2022) [31].) The identified tags are the following:

Artificial Intelligence, *Biometrics*, *Blockchain*, *Cloud Security*, *Cyber Security*, *E-Signature*, *Facial Recognition*, *Fraud Detection*, *Internet of Things*, *Intrusion Detection*, *Machine Learning*, *Network Security*, *Penetration Testing*, *Privacy*, *Private Cloud*, *QR Codes*, *Quantum Computing*, *Security*, *Spam Filtering*.

We know that Artificial Intelligence and Machine Learning cover fields beyond cybersecurity. However, we choose to include them for several reasons. First, as in other fields, they take increasing importance in cybersecurity, such as Internet traffic analysis, intrusion detection, or fraud detection. Second, this inclusion will not bias our results, as we estimate them sector-wise. Third, since the evolution of these industries is concurrent with pure cybersecurity, they also constitute an interesting benchmark better known to both the general public and VC investors. Finally, if a firm has several tags, we only include the first one, ensuring no overlap in our sectors' data.

Financial method

To compute returns from individual funding rounds to exits (acquisitions or IPOs), we account for capital dilution in the single case examined in this study. First, we calculate the equity value at the exit for an investor entered at a funding round i:

$$x_i = \underbrace{\frac{m_i}{v_i}}_{\substack{\text{initial stake}\\ \text{of investors i}}} \times \underbrace{\frac{v_i - m_{i+1}}{v_{i+1}}}_{\substack{\text{proportion of old}\\ \text{equity at round } i+1}} \times \ldots \times \underbrace{\frac{v_{n-1} - m_n}{v_n}}_{\substack{\text{proportion of old}\\ \text{equity at round } n}}$$

where $m_i, m_{i+1}, \ldots, m_n$ are the amount raised from investors at each round, $v_i, v_{i+1}, \ldots, v_n$ is the equity value at each round, and x_i is the percentage of equity owned by investors on exit. The return for these investors is

$$R_i = \frac{\overbrace{v_n \times x_i}^{\substack{\text{value owned}\\ \text{at exit}}} - m_i}{m_i}$$

Next, we use a similar approach to Cochrane (2005) [1]. We do not rely on his maximum likelihood approach, as fewer observed returns with disaggregated sectors would make the optimizer's convergence infeasible. Instead, we scale returns at the exit date by the time difference in days between the initial funding round and the observed or inferred PMV and the exit time. We obtain implicit daily arithmetic returns, which we then convert into quarterly returns. We subsequently average these returns in each sector to obtain our time series of returns. Finally, the particularly skewed distribution of VC returns imposes the use of a log model,

$$\begin{cases} \mathrm{d}\ln \mathrm{V} = (\mathrm{r^f} + \gamma)\mathrm{dt} + \delta(\mathrm{d}\ln \mathrm{V^m} - \mathrm{r^f dt}) + \sigma \mathrm{dB} \\ \mathrm{d}\ln V^m = \mu_m \mathrm{d}t + \sigma_m \mathrm{d}B^m \end{cases} \tag{1}$$

where dB is a standard Brownian motion, V is the value of the asset (firm capital), r^f is the risk-free rate, γ is the intercept, δ is the slope, V^m is the value of the market, and σ is the volatility of the value process. We follow Cochrane (2005) and assume $[B, B^m]_t = 0$ [1]. In discrete time (for a time step $\Delta t = 1$), the model is,

$$\ln\left(\frac{V_{t+1}}{V_t}\right) = \ln R^f_{t+1} + \gamma + \delta(\ln R^m_{t+1} - \ln R^f_{t+1}) + \epsilon_{t+1} \tag{2}$$

where $\epsilon_{t+1} \sim \mathcal{N}(0, \sigma^2 \Delta t)$, $R^f_{t+1} = 1 + r^f_{t+1}$, and $R^m_{t+1} = 1 + \frac{V^m_{t+1} - V^m_t}{V^m_t}$ Thus, the value of the firm V_{t+1} follows a log-normal distribution with parameters:

$$\mu_{t+1} = \ln R^f_{t+1} + \gamma + \delta(\ln R^m_{t+1} - \ln R^f_{t+1})$$
$$\sigma^2_{t+1} = \sigma^2$$

$$\mathbb{E}[\ln r] = \gamma + \mu_{\ln r_f} + \delta(\mu_{\ln r_M} - \mu_{\ln r_f}) \tag{3}$$

$$\mathbb{V}[\ln r] = \delta^2 \sigma^2_{\ln r_M} + \sigma^2 \tag{4}$$

Since we use a quarterly frequency, we multiply by four to annualize results and by 100 to get percentages. To get the results for the arithmetic returns, we take the expectation and variance of a log-normal variable, with $R = r + 1$ and $\mu = \mathbb{E}[\ln R]$:

$$\mathbb{E}[R] = \exp\left(\mu + \frac{1}{2}\sigma^2\right) - 1 \tag{5}$$

$$\mathbb{V}[R] = (\exp(\sigma^2) - 1)\exp(2\mu + \sigma^2) = (\exp(\sigma^2) - 1)(\mathbb{E}[R] + 1)^2 \tag{6}$$

We depict the model estimation process in the bottom panel of Appendix Fig. A1.

Results

Descriptive and summary statistics

Cybersecurity ventures locations

In Fig. 2, we display the share of investment raised by firms of each sector, depending on their top five locations. Unsurprisingly, the US accounts for the vast majority of this investment, with the exceptions of facial recognition, where China alone has more than 80% of the firms targeted by VC investments. This is perhaps not surprising given the massive adoption of facial recognition for its security and the implementation of the social credit system in China. The other sector vastly dominated by a non-US country is the QR codes, where India's firms alone represent 98% of the amount invested. We also try to make sense of these surprising figures, and from anecdotal evidence, we find support for massive adoption of QR codes, primarily for payment systems. (see, e.g. https://www.bloomberg.com/press-releases/2022-06-03/digital-payments-in-india). A third technology for which the US dominance is not clear is penetration testing. Indeed, whereas US firms in this industry receive 42% of the investment, it is closely followed by Israel with 41% of the funding. By the same token, whereas US privacy firms are leaders in capital raised, with 57%, Canadian firms capture a significant part of this investment with 26%. Unsurprisingly, China often reaches a second, considerable market share, with 27% for E-signature, 22% for IoT, 12% for machine learning, 19% for artificial intelligence, and 15% for biometrics firms.

Summary statistics

We report summary statistics of our data, funding amounts, and PMVs. Table 2 reports the number of firms, the number of funding rounds targeting the firms, and the average, median, total values, and standard deviations for each cybersecurity sector's funding amount and PMVs. The top three amounts raised over 2010–2022 are the artificial intelligence, security, and machine learning sectors, with USD 124.3, 67.5, and 67.3 bln, respectively. We know these three sectors might include more firms than those using these technologies for cybersecurity reasons, particularly artificial intelligence and machine learning. Regarding security, however, the fact that Crunchbase is heavily tilted toward tech companies, together with a manual sampling of the firms to check their actual businesses, makes us confident that many relate to cybersecurity. They also dominate the ranking in funding rounds events, with up to 6339 rounds recorded for the artificial intelligence sector. The following category in this ranking is the more specific cybersecurity category, with around USD 40 billion raised over the last decade, followed by blockchain, which has over USD 27 billion. Once again, for this latter category, we are aware of the biases that may be induced by cryptocurrencies and NFT companies that do not relate to the pure cybersecurity sector. However, the technology itself is tightly connected to it, and Crunchbase has other denominations for pure financial-related projects in the space, such as "Cryptocurrency," "Bitcoin," or "Ether." The private cloud sector vastly dominates other sectors in terms of average (USD 45.46 mln) and median funding (USD 11 mln). Following the average funding criterion, it is followed by QR codes (USD 37.76 mln), facial recognition (USD 31.48 mln), and cloud security (USD 25.23 mln). In-

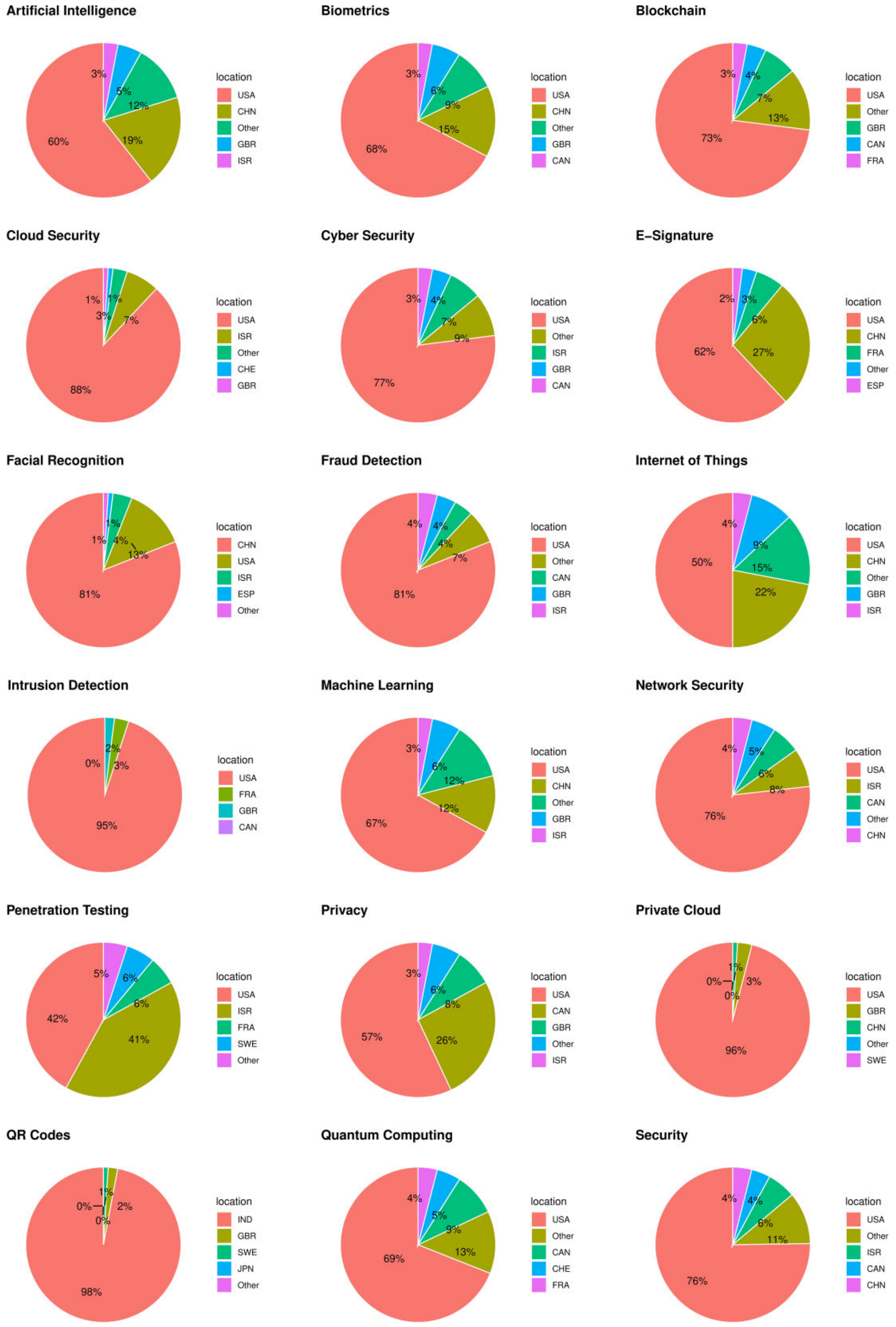

Figure 2. Location repartition of funded firms' capital raised in cybersecurity sectors. This figure reports the share of funding amount per country where the firms raising capital have their headquarters. We report the top four locations ranked by funding amount and aggregate all the others in an "Other" category. We do not report the spam filtering sector since we find in the dataset that it is 100% US-based. The period of observations is 2010–2022.

Table 2. Descriptive statistics of funding amount PMVs for cybersecurity sectors.

		Funding amount				PMVs			
Sectors	#Rounds	Avg.	Median	Total	SD	Avg.	Median	Total	SD
Artificial intelligence	6339	19.60	4.10	124 256.80	79.64	151.64	21.21	961 248.10	686.76
Biometrics	130	10.96	3.80	1425.26	28.50	67.26	20.00	8743.24	200.00
Blockchain	1392	19.47	3.10	27 104.71	71.19	199.31	18.70	277 443.60	891.12
Cloud security	502	25.23	10.00	12 664.88	47.17	206.52	48.81	103 671.70	564.79
Cyber security	1759	22.71	8.42	39 946.45	49.50	202.40	39.31	356 017.50	655.71
E-signature	41	16.97	2.23	695.79	48.93	132.17	11.23	5418.92	476.42
Facial recognition	60	31.48	3.85	1888.50	114.33	201.32	17.43	12 078.95	646.72
Fraud detection	223	26.72	8.00	5959.54	74.31	251.16	39.04	56 009.71	1388.45
Internet of Things	1768	12.73	3.00	22 507.51	42.35	87.04	16.75	153 880.50	287.91
Intrusion detection	29	24.50	11.00	710.52	50.72	303.36	51.80	8797.36	730.08
Machine learning	3974	16.93	4.50	67 288.87	48.17	134.42	22.50	534 165.90	474.34
Network security	1034	21.71	10.00	22 448.87	43.03	170.78	46.97	176 586.40	442.26
Penetration testing	28	14.54	5.67	407.06	28.20	89.31	33.21	2500.68	191.99
Privacy	238	18.03	5.35	4291.04	48.61	158.94	27.43	37 827.69	613.25
Private cloud	63	45.46	11.00	2863.77	108.43	447.22	56.84	28 174.61	1406.49
QR codes	17	37.76	2.00	641.88	86.38	300.61	10.71	5110.34	695.72
Quantum computing	78	21.41	9.74	1669.95	53.79	142.90	44.06	11 146.37	381.99
Security	3551	19.02	7.51	67 543.82	41.89	153.43	35.33	544 825.10	501.43
Spam filtering	8	7.24	6.25	57.90	6.41	32.39	26.88	259.14	28.36
Total cybersecurity	21 234	19.04	5.00	404 373.10	60.36	154.65	26.19	3 283 906.00	609.43
Information technology	74 002	23.06	5.05	1 706 460.00	145.71	165.83	25.31	12 271 484.00	707.27
Health	4644	19.09	3.14	88 644.37	95.62	130.40	17.53	605 590.00	661.96
Retail	9586	19.58	3.41	187 738.80	72.74	163.39	18.56	1 566 300.00	803.58
Other	31 653	29.77	6.80	942 417.50	156.78	201.64	33.45	6 382 453.00	729.94

This table reports the number of funding rounds and average, median, total, and standard deviation estimates for the funding amount and PMVs regarding the 19 cybersecurity sectors and four aggregated other sectors: Information technology (excluding cybersecurity sectors), Health, Retail, and Others. The values are in USD mln, and the study period is 2010–2022.

stead, spam filtering, biometrics, and IoT close this ranking, with an average funding of USD 7.24, 10.96, and 12.73 mln, respectively. Given the significant heterogeneity across cybersecurity sectors in terms of the number of rounds, average funding, and total capital raised, our findings support the view that investments differ across sub-sectors. When considered in aggregate, the cybersecurity sector accounts for 21 234 rounds or about 28% of the IT sector (excluding all aforementioned cybersecurity sub-sectors). The share of cybersecurity over the rest of IT comes to similar values, with 23% and 27% for total funding and PMVs, respectively. Regarding average funding, the broad cybersecurity sector gets an average deal size of USD 19.04 mln, which is slightly lower than IT and the same size as the Health and Retail sectors. Compared to other broader sectors, such as Health and Retail, Crunchbase's tilt toward technology stocks is also evident, with only 4644 and 9586 recorded funding rounds for the Health and Retail sectors, respectively.

The total PMVs are approximately one order of magnitude larger than the funding amount, which is typical of the VC sector. The sectors' rankings for PMVs are similar to those of the total funding amount, albeit with some differences. Again, in this case, artificial intelligence and machine learning represent the most prominent sectors, with a total of PMVs recorded throughout the period at the trillion USD order of magnitude. However, this statistic should be interpreted with caution in this case, as it may report the sequences of several valuations provided over the company lifecycle. In contrast to the funding descriptive statistics, the private cloud sector ranks first, with an average firm PMVs of USD 447.22 mln, followed by the intrusion detection sector (USD 303.36 mln), QR codes (USD 300.61), and fraud detection (USD 251.16 mln). The average PMVs of cybersecurity firms (USD 26.19 mln) and those of IT (USD 25.31 mln) are indistinguishable. However, both are much more extensive than the health and retail sectors. For the average company in the cybersecurity sector, one dollar invested translates into up to ten dollars in PMVs. These 10-fold returns between two funding rounds are typically in the order of magnitude that VC funds advertise. However, these substantial returns should be taken cautiously due to the large standard deviations associated with the valuations of these categories. For instance, for the private cloud and fraud detection sectors, it is USD 1406 mln and USD 1338 mln, respectively. Second, our data almost surely come with a selection bias and an over-representation of "unicorns."

Nonetheless, we do not see any fundamental reason why this selection bias should not be uniformly distributed across categories. Thus, the ranking we observe should represent the relative performance of each sector. Overall, we find that the valuations of cybersecurity firms vary significantly depending on the industry to which they belong. These findings strongly support the view that valuations are sub-sector-specific. In Tables A2 and A3 of the appendix, we also report the results of pairwise t-tests that compare the relative performance of sectors' funding amounts and PMVs. Finally, we find a substantial standard deviation associated with PMVs in all industries. Although the observations of valuations do not align with our methodology for computing returns from funding rounds to exits, they further justify using a market model to adjust returns, combined with a log model in the subsequent analysis.

Table 3. Descriptive statistics of time to exit and number of investors for cybersecurity sectors.

	Time to exit (days)				Number of investors	
Sectors	Avg.	SD	Max	Min	Avg.	SD
Artificial Intelligence	1702	883	3971	52	3.69	3.84
Biometrics	1749	1151	4011	196	4.20	3.41
Blockchain	1085	691	2899	65	3.70	3.72
Cloud Security	1926	991	4120	260	3.84	3.50
Cyber Security	1880	968	3702	119	3.71	3.75
E-Signature	1186	1005	2346	595	4.33	3.62
Facial Recognition	1156	580	1985	202	4.01	3.38
Fraud Detection	1874	1257	3085	166	3.70	3.26
Internet of Things	1579	859	3738	7	3.65	3.65
Intrusion Detection	1986	1265	2881	1092	2.84	2.88
Machine Learning	1775	853	3902	82	3.76	3.88
Network Security	1932	929	3913	132	3.69	4.15
Penetration Testing	NA	NA	NA	NA	5.03	4.31
Privacy	1002	782	3022	31	3.90	3.82
Private Cloud	1995	1036	3608	206	3.94	3.23
QR Codes	NA	NA	NA	NA	5.68	3.16
Quantum Computing	1962	397	2252	1528	2.80	2.92
Security	1774	931	3427	106	3.81	4.06
Spam Filtering	1574	649	1949	825	4.00	4.50
Total cybersecurity	1747	1356	4120	7	3.46	3.60
Information technology	1353	852	4418	15	3.06	3.10
Health	1237	781	4169	37	3.75	3.72
Retail	1352	877	4290	122	3.72	3.90
Other	1256	867	4479	52	3.25	3.21

This table reports descriptive statistics about the time to exit (means, standard deviations, maximum and minimum time). We discard the sectors with less than 10 IPO observations. It also reports the means and standard deviations of the number of investors. The study period is 2010–2022.

Characteristics and time to success

Table 3 reports the average, standard deviation, maxima, and minima of the time to IPO from the first funding round observation available from 2010 onward (we thank an anonymous referee of The 22nd Workshop on the Economics of Information Security (WEIS) for suggesting this table). With 1995 days on average, the private cloud sector is the longest to reach an exit from the first recorded funding round, with intrusion detection, cloud security, and quantum computing in the same range. Instead, the blockchain, e-signature, facial recognition, and privacy sectors take less than 3 years on average to reach an exit. Firms from the broader IT sector (excluding cybersecurity firms) are faster by over 1 year (1747 vs 1353 days) to reach exit than those of the cybersecurity sector. In that aspect, IT firms appear very similar to firms from the more traditional sectors, such as health and retail, whose time to exit ranges between 1237 and 1256 days. Thus, cybersecurity firms could, globally, take slightly longer to reach maturity. We also present the average number of investors per round, for which the cross-sectional variations are much more limited. For instance, whereas the sector with the highest average number of investors is five (penetration testing), the sector with the lowest number is about three (intrusion detection). However, this exercise is limited by the fact that many firms have not experienced an IPO or buyout in the sample yet, and some sectors could face a dramatic change in terms of exits given their relatively recent success, such as artificial intelligence and the surge of generative models. Interestingly, the average number of investors in cybersecurity firms is slightly higher than for IT ones (3.46 vs 3.06) and comes closer to traditional businesses of health, retail, and other sectors (from 3.25 to 3.75).

Financial performance of cybersecurity ventures

Log model regressions

Using Cochrane's (2005) approach, we compute the returns to exit, accounting for capital dilution across firms' lifecycle. Next, we set up a three-month grid to average returns on each sector. We match the quarterly returns on the S&P 500 and the risk-free rate observations at the quarterly frequency and estimate the log model of Eq. 2. Thus, we must discard technologies for which there are not enough observations to estimate the model or, more importantly, that are not sufficiently spread over 2010–2022. We are left with 12 sectors. In Table 4, we report the results of the parameters' estimations, γ, δ, and σ, as well as the implied parameters α and β for the arithmetic form. We find α, the return in excess of the market risk premium, to be positive for all technologies. Even though we cannot compute the standard errors for these implied parameters, the corresponding parameter in the log model γ is significant at the 1% level for nine sectors, except privacy and private cloud (5% level significance) and blockchain (non-statistically significant). In terms of size, this intercept translates into between 4.28% (network security) and 5.16% (blockchain) of annualized risk-adjusted returns. The δ parameter is not statistically significant at the usual levels, except for privacy, at the 1% level. The implied parameter β ranges between 0.51 for biometrics and 5.51 for privacy. This parameter reflects the covariance of the selected sector with the index. It evaluates the systematic risk to which the sector is exposed in the standard Capital Asset Pricing Model framework. The larger this coefficient, the higher the expected returns, everything being equal. This parameter also provides information about the sector's cyclicality in the broad economy. The larger (smaller) the coefficient, the more pro-(contra-) cyclical the sector is.

Table 4. Estimates for the log model regressions and the implied values for α and β.

Sector	γ	se(γ)	δ	se(δ)	σ (%)	α	β
Artificial intelligence	0.13***	0.03	0.48	0.47	31.24	1.14	1.62
Biometrics	0.07***	0.02	−0.68	0.63	5.24	1.08	0.51
Blockchain	0.26	0.20	−0.26	8.95	91.80	1.29	0.77
Cloud security	0.11***	0.01	0.25	0.19	11.24	1.12	1.28
Cyber security	0.08***	0.01	−0.32	0.18	13.71	1.08	0.73
E-signature	0.08**	0.04	0.49	1.02	6.73	1.09	1.63
Fraud detection	0.13***	0.05	−0.56	0.73	17.33	1.14	0.57
Internet of Things	0.07***	0.02	−0.35	0.35	20.31	1.08	0.71
Machine learning	0.13***	0.02	0.15	0.30	19.13	1.13	1.17
Network security	0.07***	0.01	−0.20	0.21	14.79	1.07	0.82
Privacy	0.12**	0.05	1.71***	0.65	17.74	1.13	5.51
Private cloud	0.12**	0.06	−0.12	0.74	15.38	1.13	0.88
Total cybersecurity	0.07***	0.02	0.48***	0.03	14.18	1.07	1.62
Information technology	0.23***	0.01	1.65***	0.10	46.47	0.90	1.81
Health	0.21***	0.02	0.93***	0.21	23.82	0.61	0.98
Retail	0.22***	0.01	1.72***	0.08	36.07	0.75	1.86
Other	0.20***	0.00	0.60***	0.01	48.34	0.82	0.64

This table reports the estimations of the parameters from regression of excess quarterly log-returns on the market risk premium, approximated by the excess returns of the S&P 500 on the risk-free rate (see Eq. 2), for 12 cybersecurity sectors, and four higher-level sectors for comparison: Information technology (excluding cybersecurity sectors), Health, Retail, and Other. We report the exact standard errors for the Υ and δ parameters and the total volatility in percentage. We also report the α and β parameters, equivalent of Υ and δ in the model in arithmetic form. ***, **, * indicates significance at the 1%, 5%, and 10% levels, respectively. The period of observations is 2010–2022.

This is particularly important for cybersecurity as, similar to other sectors that mitigate crises, it tends to be more counter-cyclical. One anecdotal evidence is the performance of the pharmaceutical sector in the COVID crisis. As the broad economy collapsed, pharmaceutical companies experienced, on average, high returns with COVID treatment prospects.

With this consideration, artificial intelligence, with β over 1.62, is mainly pro-cyclical, which is not surprising given the non-exclusivity of this sector for cybersecurity. In sharp contrast, making sense of privacy's outstandingly high β is complex. We can only posit that privacy matters more in good economic conditions without assuming any causal link. Instead, firms for which cybersecurity activity is more explicit, those tagged as cybersecurity, network security, fraud detection, and private cloud, have β well below one. These results imply that these sectors are less procyclical than others and would perform better or "less worse" in market depression. Considering the overall cybersecurity sector, we find a β of 1.62, which supports the view of a high procyclicality. However, it remains well below that of the IT sector (1.81) or the retail sector (1.86). An overall larger contra-cyclicality could be justified for cybersecurity if firms indeed took immediate measures to invest in such measures around cyber incidents to mitigate these costs. However, the consensus in the related literature tends to support two views that go against this principle. First, firms under-invest in cybersecurity; an immediate cybersecurity investment is unlikely to follow a cyber-incident. Second, the actual impact of cyber-incidents on firms' value is found to be insignificant; see, e.g. Gordon et al. [32]. The health sector ($\beta = 0.98$) is a good counter-example, with an industry that is almost insensitive to customers' revenues (they will prioritize health over other expenses). Which in times of health crises would instead rise up while the market goes down (this is out of the scope of this research, but since our sample ends in 2022, the health sector, particularly low β likely incorporates some aspects of the COVID crisis with higher valuations when the market underperformed). Cochrane (2005) additionally finds that the aggregate level of systematic risk, corresponding to the β parameter, is 1.9 for the whole VC market and ranges across industries between −0.1 (retail) and 1.7 (IT) [1]. We find similar values, with 1.62 on an aggregate, and the range of systematic risk across sub-sectors falls in the same range, except for privacy. Ewens (2009) finds values slightly closer to ours, with a beta of 2.4 and an annualized alpha of 27% [3]. Finally, Peng (2004) finds an average return of 55.18% per year and an index β with the S&P 500 of 2.4, closer to our results [14]. Thus, if VC markets behave similarly across the period, our results would support the view that cybersecurity sectors are intrinsically different from the broader VC investment class.

Implied expected returns

Table 5 presents the expectation and standard errors for log returns computed with Eqs. 3, 4, and the corresponding one for the arithmetic returns computed with Eqs. 5, 6. The blockchain sector reaches annual expected arithmetic (log) returns of 177.27% (105.42%), which is in line with the underlying performance of cryptocurrencies over the 2010-2022 period. The second in this ranking is artificial intelligence, with annualized returns of 67.25%, in line with the results of Cochrane (2005) for IT (79%). Other sectors in the high range include machine learning (58.5% p.a.), private cloud (57.88% p.a.), and cloud security (50.58% p.a.). We find substantial heterogeneity across sectors regarding systematic risks (β from 0.71 to 5.51) and expected returns (from 9.72% p.a. to 177.27% p.a.). In contrast, we find that risk-adjusted returns (annualized α from 4.28% to 5.16%) lie in a tight range. Together with their relatively small sizes, as opposed to unadjusted returns, this also points to correct pricing for broad cybersecurity. Overall, the total risk, risk-adjusted returns, expected returns, and systematic risks differ vastly across sectors. Finally, the fact that all risk-adjusted returns are positive points to the overall attractiveness of the cybersecurity industry.

Compared to previous findings of the VC literature, the cybersecurity industry stands out. Cochrane (2005) finds an average annualized arithmetic return of 59% for all industries combined, ranging from 42% for the health sector to 111% for the retail sector [1]. Almost 20 years later and with a different database, we obtain expected returns of 44.40% for IT, 28.84% for health, and 38.65% for the retail sector. Thus, returns on the cybersecurity industry are lower than

Table 5. Implied estimates for $\mathbb{E}[\ln R]$, and $\mathbb{E}[R]$.

Sector	E[ln R]	se(E[ln R])	E[R]	se(E[R])
Artificial intelligence	55.55	14.62	67.25	16.85
Biometrics	31.30	4.72	23.22	2.55
Blockchain	105.42	42.15	177.27	64.14
Cloud security	47.21	5.37	50.58	5.81
Cyber security	33.09	6.57	36.40	6.87
E-signature	36.10	4.25	48.54	3.46
Fraud detection	54.99	8.63	46.34	8.89
Internet of Things	31.87	9.55	37.77	10.23
Machine learning	52.57	8.83	58.50	10.09
Network security	29.41	6.89	31.81	7.34
Privacy	51.89	13.07	9.72	8.35
Private cloud	50.81	7.09	57.88	8.09
Total cybersecurity	34.17	8.48	37.43	6.94
Information technology	30.45	48.28	44.40	54.43
Health	24.74	24.93	28.84	26.83
Retail	29.46	38.56	38.65	42.68
Other	23.05	48.58	36.41	53.79

This table reports the implied estimates for the expected value and standard errors computed from the log and arithmetic models with quarterly returns in 12 cybersecurity sectors and four higher-level sectors: Information technology (excluding cybersecurity sectors), Health, Retail, and Other. We annualize the values and display them in percentages. The study period is 2010–2022.

those of IT, with only 37%. However, compared individually, some sub-sectors, such as artificial intelligence and blockchain, reach the top of this range or completely dominate it.

Conclusion

This research provides an in-depth examination of the financial performance of private firms across 19 cybersecurity sectors identified in Crunchbase, covering the period from 2010 to 2022. By analyzing funding rounds, valuations, and exit events, we aim to highlight the growth potential within the cybersecurity industry. Given data gaps in Crunchbase, we employ machine learning techniques to estimate missing valuations, facilitating a more comprehensive assessment. Additionally, we apply Cochrane's (2005) approach to compute returns accounting for capital dilution, recognizing that multiple funding rounds are standard in the VC context [1]. Our findings show that artificial intelligence, security, and machine learning lead in capital raised, each attracting over USD 60 bln. However, the private cloud sector ranks highest in terms of average and median PMVs, with firms achieving an average of up to USD 45.46 million. Our analysis indicates that while the cybersecurity industry's average funding and PMVs lag behind the broader IT sector, the time to exit for cybersecurity firms remains notably longer, suggesting unique challenges to market maturity.

Further analysis using a log return process reveals that all cybersecurity sectors exhibit positive alpha (excess returns above the market risk premium). In contrast, beta (systematic risk) values range from 0.51 to 5.51, with cybersecurity firms displaying slightly lower cyclicality than IT firms. Among sectors, artificial intelligence and blockchain show the highest expected arithmetic and log returns, with blockchain reaching an annualized return of 177.27%, likely influenced by trends in cryptocurrency. In contrast, sectors such as privacy and biometrics yield lower expected returns. Overall, our research uncovers substantial performance variations among cybersecurity sectors in terms of funding, valuations, cyclicality, and adjusted returns. Notably, compared to IT, cybersecurity firms exhibit signs of undervaluation, characterized by lower funding, longer exit timelines, less procyclicality, and lower expected returns. These characteristics may partially explain the sector's slower capital influx and highlight potential reasons for under-investment by investors and customers, despite cybersecurity's critical role in technology ecosystems worldwide.

Acknowledgments

We appreciate helpful comments from seminar participants at the Cyber Alp Retreat 2022 and WEIS 2023.

Author contributions

Loïc Maréchal (Conceptualization, Data curation, Methodology, Software, Visualization, Writing–original draft, Writing – review & editing), Alain Mermoud (Conceptualization, Investigation, Project administration, Validation), Dimitri Percia David (Formal analysis, Validation, Writing – review & editing), Mathias Humbert (Conceptualization, Investigation, Project administration, Validation, Writing – review & editing)

Conflict of interest: None declared.

Funding

This document results from a research project funded by the Cyber-Defence Campus, armasuisse Science and Technology.

Appendix

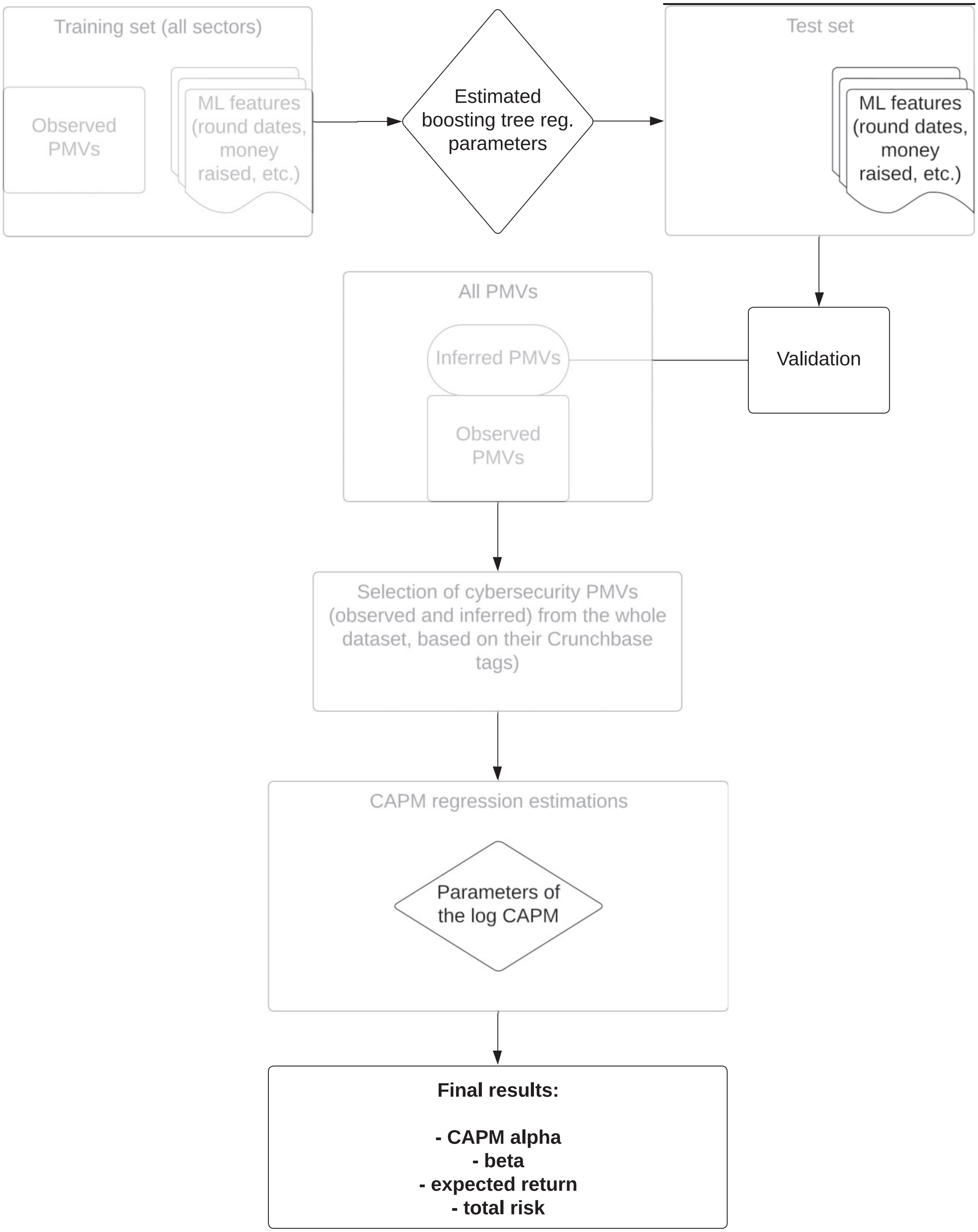
Training set (all sectors)
Observed PMVs
ML features (round dates, money raised, etc.)
Estimated boosting tree reg. parameters
Test set
ML features (round dates, money raised, etc.)
Validation
All PMVs
Inferred PMVs
Observed PMVs
Selection of cybersecurity PMVs (observed and inferred) from the whole dataset, based on their Crunchbase tags)
CAPM regression estimations
Parameters of the log CAPM
Final results:
- CAPM alpha
- beta
- expected return
- total risk

Figure A1. Flowchart of data interpolation and processing. This figure details the data treatment process from the data interpolation with the boosting tree regression approach trained on all Crunchbase data, not only cybersecurity firms, then selected according to Crunchbase cybersecurity-related tags and treated with a log-CAPM approach to yield the final arithmetic CAPM estimates.

Table A1. Examples of firms included in each of the 19 selected sectors. This table reports a randomly selected company for each sector and details its name, an excerpt of the business description provided by the firm, website, and country.

Sector	Company name	Excerpt of business description	Website	Country
Artificial Intelligence	Alation, Inc.	"Data intelligence platform."	http://alation.com	USA
Biometrics	Gingko Bioworks	"Enzyme, proteins, or biosecurity services."	https://www.ginkgobioworks.com	USA
Blockchain	Procivis GmbH	"Decentralised data storage, self-sovereignty over personal data."	https://www.procivis.ch	Switzerland
Cloud Security	Perpecsys	"Cloud computing security."	http://perspecsys.com	Canada
Cyber Security	Smart Hive	"allows organizations to learn from each other anonymously in 90 seconds or less."	https://www.smarthive.io	USA
E-Signature	Oneflow AB	"Automate the entire contract process - from creating to signing and managing."	https://oneflow.com	Sweden
Facial Recognition	Clearview AI, Inc.	"...allows law enforcement to rapidly generate leads to help identify suspects, witnesses and victims."	https://www.clearview.ai	USA
Fraud Detection	Ravelin Ltd.	"...reduce your chargeback rate and stop fraudsters in their tracks using both machine learning and human insights."	http://www.ravelin.com	UK
Internet of Things	Zuli	"Connect your lights and appliances to Zuli Smartplugs, control them from one app..."	https://zuli.io	USA
Intrusion Detection	Cybereason, Inc.	"We deliver the precision to end cyber attacks in an instant - on computers, mobile devices, servers, and in the cloud."	https://www.cybereason.com	USA
Machine Learning	Vidrovr	"Using machine learning, Vidrovr processes messy unstructured video, image, or audio data..."	https://www.vidrovr.com	USA
Network Security	Perimeter 81	"Easily deploy, manage, and scale a secure corporate network without compromising performance."	https://www.perimeter81.com	Israel
Penetration Testing	Bugcrowd, Inc.	"Penetration testing as a service (PTaaS) done right."	https://bugcrowd.com	USA
Privacy	Anonyome Labs, Inc.	"We provide scalable mobile and desktop solutions that empower users to protect their private information."	https://anonyome.com	USA
Private Cloud	Zerto Ltd.	"Private, hybrid, and multi-cloud."	http://www.zerto.com	USA
QR Codes	Supercode	"Supercode is a professional QR code creation platform for businesses."	https://supercode.com	USA
Quantum Computing	blueqat, Inc.	"blueqat Inc. is a quantum machine learning company based in Shibuya, Tokyo."	https://blueqat.com	Japan
Security	Paladin Drones	"Drone as a first responder (DFR) technology giving first responders a live overhead view before they arrive on scene."	https://paladindrones.io	USA
Spam Filtering	Two Hat Security Ltd.	"The world's leading content moderation solution."	https://www.twohat.com	Canada

Table A2. T-tests of unequal variances of funding amount for each category. This table reports t-statistics for pairwise mean t-tests of funding amount per sector. The t-statistics correspond to tests for unequal (Welch's t-tests) variance. The values are computed by comparing the row-wise to the column-wise entries.

Sectors/Sectors	AI	BI	BL	CS	CS	E-S	FR	FD	IoT	ID	ML	NS	PT	PR	PC	QR	QC	S	SF
Artificial Intelligence		3.21	0.06	−2.41	−2.01	0.34	−0.80	−1.40	4.84	−0.52	2.12	−1.26	0.93	0.48	−1.89	−0.87	−0.29	0.48	4.99
Biometrics	−3.21		−2.71	−4.36	−4.25	−0.75	−1.37	−2.83	−0.66	−1.39	−2.28	−3.79	−0.61	−1.76	−2.48	−1.27	−1.59	−3.10	1.10
Blockchain	−0.06	2.71		−2.03	−1.44	0.32	−0.81	−1.36	3.12	−0.52	1.24	−0.96	0.87	0.39	−1.88	−0.87	−0.30	0.22	4.13
Cloud Security	2.41	4.36	2.03		1.04	1.04	−0.42	−0.28	5.35	0.08	3.70	1.41	1.87	1.90	−1.46	−0.60	0.59	2.80	5.82
Cyber Security	2.01	4.25	1.44	−1.04		0.74	−0.59	−0.79	6.43	−0.19	4.11	0.56	1.50	1.39	−1.66	−0.72	0.21	2.68	6.06
E-Signature	−0.34	0.75	−0.32	−1.04	−0.74		−0.87	−1.07	0.55	−0.62	0.005	−0.61	0.26	−0.13	−1.82	−0.93	−0.45	−0.27	1.22
Facial Recognition	0.80	1.37	0.81	0.42	0.59	0.87		0.31	1.27	0.40	0.98	0.66	1.08	0.89	−0.70	−0.25	0.63	0.84	1.62
Fraud Detection	1.40	2.83	1.36	0.28	0.79	1.07	−0.31		2.76	0.21	1.95	0.97	1.67	1.48	−1.29	−0.51	0.68	1.53	3.56
Internet of Things	−4.84	0.66	−3.12	−5.35	−6.43	−0.55	−1.27	−2.76		−1.24	−3.32	−5.36	−0.33	−1.60	−2.39	−1.19	−1.41	−5.12	2.22
Intrusion Detection	0.52	1.39	0.52	−0.08	0.19	0.62	−0.40	−0.21	1.24		0.80	0.29	0.92	0.65	−1.26	−0.58	0.28	0.58	1.78
Machine Learning	−2.12	2.28	−1.24	−3.70	−4.11	−0.005	−0.98	−1.95	3.32	−0.80		−3.10	0.44	−0.34	−2.08	−0.99	−0.73	−2.01	4.06
Network Security	1.26	3.79	0.96	−1.41	−0.56	0.61	−0.66	−0.97	5.36	−0.29	3.10		1.31	1.08	−1.73	−0.76	0.05	1.78	5.50
Penetration Testing	−0.93	0.61	−0.87	−1.87	−1.50	−0.26	−1.08	−1.67	0.33	−0.92	−0.44	−1.31		−0.56	−2.11	−1.07	−0.85	−0.83	1.26
Privacy	−0.48	1.76	−0.39	−1.90	−1.39	0.13	−0.89	−1.48	1.60	−0.65	0.34	−1.08	0.56		−1.96	−0.93	−0.49	−0.31	2.78
Private Cloud	1.89	2.48	1.88	1.46	1.66	1.82	0.70	1.29	2.39	1.26	2.08	1.73	2.11	1.96		0.31	1.61	1.93	2.76
QR Codes	0.87	1.27	0.87	0.60	0.72	0.93	0.25	0.51	1.19	0.58	0.99	0.76	1.07	0.93	−0.31		0.75	0.89	1.45
Quantum Computing	0.29	1.59	0.30	−0.59	−0.21	0.45	−0.63	−0.68	1.41	−0.28	0.73	−0.05	0.85	0.49	−1.61	−0.75		0.39	2.18
Security	−0.48	3.10	−0.22	−2.80	−2.68	0.27	−0.84	−1.53	5.12	−0.58	2.01	−1.78	0.83	0.31	−1.93	−0.89	−0.39		4.97
Spam Filtering	−4.99	−1.10	−4.13	−5.82	−6.06	−1.22	−1.62	−3.56	−2.22	−1.78	−4.06	−5.50	−1.26	−2.78	−2.76	−1.45	−2.18	−4.97	

Table A3. Cybersecurity sectors pairwise comparison of the average PMVs. This table reports t-statistics for pairwise mean t-tests of PMVs per sector. The t-statistics correspond to tests for unequal (Welch's t-tests) variance. The values are computed by comparing the row-wise to the column-wise entries, and the period is 2010–2022.

Sectors/Sectors	AI	BI	BL	CS	CS	E-S	FR	FD	IoT	ID	ML	NS	PT	PR	PC	QR	QC	S	SF
Artificial Intelligence		1.63	2.32	−9.56	−12.89	1.29	0.42	−6.46	7.31	−3.27	−0.56	−13.99	−0.45	−3.42	−3.80	0.66	−2.96	−12.13	0.03
Biometrics	−1.43		−0.69	−6.27	−5.75	0.48	−0.46	−5.40	0.81	−3.67	−1.77	−6.57	−1.11	−3.42	−4.15	0.36	−3.38	−4.70	−0.68
Blockchain	−2.36	0.61		−9.76	−11.33	0.86	−0.11	−7.06	3.39	−3.65	−2.58	−12.54	−0.87	−4.27	−4.23	0.50	−3.55	−9.87	−0.40
Cloud security	9.08	5.98	9.39		1.87	3.72	3.45	0.26	12.76	−0.72	9.13	0.34	2.03	3.16	−0.82	1.63	1.07	4.04	2.53
Cyber security	12.42	5.39	11.44	−1.88		3.27	2.90	−1.08	16.31	−1.27	11.79	−2.11	1.54	2.20	−1.47	1.42	0.27	3.39	2.05
E-signature	−1.36	−0.53	−0.89	−4.10	−3.67		−0.75	−3.49	−0.14	−3.24	−1.36	−3.69	−1.24	−2.36	−3.47	0.16	−2.67	−2.73	−0.90
Facial recognition	−0.43	0.49	0.11	−3.66	−3.13	0.75		−3.16	1.01	−2.83	−0.51	−3.43	−0.62	−1.77	−3.09	0.51	−2.16	−2.23	−0.25
Fraud detection	5.89	5.34	6.47	−0.26	1.05	3.88	3.37		9.11	−0.81	6.22	−0.04	1.85	2.45	−0.92	1.57	0.83	2.58	2.34
Internet of Things	−7.15	−0.75	−3.41	−12.61	−16.30	0.15	−1.07	−8.70		−4.39	−7.33	−17.18	−1.60	−6.39	−5.10	0.22	−4.75	−15.66	−1.14
Intrusion detection	2.92	3.73	3.20	0.69	1.21	3.14	2.71	0.80	4.08		3.20	0.84	2.00	1.97	0.01	1.79	1.24	1.83	2.36
Machine learning	0.55	1.60	2.65	−8.94	−11.64	1.48	0.53	−5.86	7.31	−2.95		−13.01	−0.39	−3.19	−3.72	0.69	−2.84	−10.57	0.10
Network security	12.27	6.79	12.17	−0.36	2.05	4.60	4.09	0.04	16.54	−0.89	11.92		1.97	3.31	−0.96	1.59	0.96	5.45	2.48
Penetration testing	0.40	1.11	0.74	−1.89	−1.43	1.19	0.59	−1.80	1.45	−2.00	0.35	−2.05		−0.70	−2.15	0.78	−1.18	−0.99	0.34
Privacy	3.00	3.42	3.81	−3.07	−2.07	2.71	1.95	−2.45	5.91	−2.02	2.90	−3.40	0.71		−2.26	1.11	−0.91	−0.71	1.18
Private cloud	4.27	4.53	4.62	0.95	1.74	3.43	3.08	1.03	5.90	−0.01	4.31	1.25	1.95	2.62		1.82	1.37	2.12	2.54
QR codes	−1.17	−0.61	−0.86	−2.92	−2.67	−0.19	−0.69	−2.76	−0.40	−2.11	−1.26	−3.29	−0.91	−2.02	−2.35		−1.33	−1.21	−0.61
Quantum computing	2.65	3.41	3.15	−1.03	−0.26	2.81	2.20	−0.82	4.44	−1.24	2.64	−1.02	1.16	0.92	−1.41	2.00		0.62	1.61
Security	11.79	4.53	10.41	−4.17	−3.43	3.18	2.50	−2.58	15.99	−1.80	10.53	−5.22	0.96	0.69	−2.62	2.37	−0.61		1.50
Spam filtering	−0.01	0.39	0.18	−1.27	−1.01	0.55	0.14	−1.26	0.55	−1.66	−0.05	−1.38	−0.25	−0.65	−1.35	0.44	−0.95	−0.76	

References

1. Cochrane JH. The risk and return of venture capital. *J Financ Econ* 2005;**75**:3–52. https://doi.org/10.1016/j.jfineco.2004.03.006
2. Gornall W, Strebulaev IA. Squaring venture capital valuations with reality. *J Financ Econ* 2020;**135**:120–43. https://doi.org/10.1016/j.jfineco.2018.04.015
3. Ewens M. A new model of venture capital risk and return. 2009. https://doi.org/10.2139/ssrn.1356322 (25 March 2022, date last accessed).
4. Korteweg A, Nagel S. Risk-adjusting the returns to venture capital. *J Financ* 2016;**71**:1437–70. https://doi.org/10.1111/jofi.12390
5. Moskowitz TJ, Vissing-Jørgensen A. The returns to entrepreneurial investment: A private equity premium puzzle? *Am Econ Rev* 2002;**92**:745–78. https://doi.org/10.1257/00028280260344452
6. Axelson U, Martinovic M. European venture capital: Myths and facts. 2015. https://personallseacuk/axelson/ulf_files/EuroVC_MythsFacts%20v17pdf
7. Franzoni F, Nowak E, Phalippou L. Private equity performance and liquidity risk. *J Financ* 2012;**67**:2341–73. https://doi.org/10.1111/j.1540-6261.2012.01788.x
8. Driessen J, Lin TC, Phalippou L. A new method to estimate risk and return of nontraded assets from cash flows: The case of private equity funds. *J Financ Quant Anal* 2012;**47**:511–35. https://doi.org/10.1017/S0022109012000221
9. Ang A, Chen B, Goetzmann WN,. *et al*. Estimating private equity returns from limited partner cash flows. *J Financ* 2018;**73**:1751–83. https://doi.org/10.1111/jofi.12688
10. Cumming D, Dai N. Fund size, limited attention and valuation of venture capital backed firms. *J Empir Financ* 2011;**18**:2–15. https://doi.org/10.1016/j.jempfin.2010.09.002
11. Cumming D, Dai N. Local bias in venture capital investments. *J Empir Financ* 2010;**17**:362–80. https://doi.org/10.1016/j.jempfin.2009.11.001
12. Engel D, Keilbach M. Firm-level implications of early stage venture capital investment - An empirical investigation. *J Empir Financ* 2007;**14**:150–67. https://doi.org/10.1016/j.jempfin.2006.03.004
13. Korteweg A, Sorensen M. Risk and return characteristics of venture capital-backed entrepreneurial companies. *Rev Financ Stud* 2010;**23**:3738–72. https://doi.org/10.1093/rfs/hhq050
14. Peng L. Building a venture capital index. 2001. http://dxdoiorg/102139/ssrn281804 (12 May 2022, date last accessed).
15. Hwang M, Quigley JM, Woodward SE. An index for venture capital, 1987–2003. *Contrib Econ Anal Policy* 2005;**4**:1–43. https://doi.org/10.2202/1538-0645.1180
16. Schmidt DM. Private equity versus stocks. *J Alternative Investments* 2006;**9**(1):28–47. https://doi.org/10.3905/jai.2006.640265
17. Cumming D, Haß LH, Schweizer D. Private equity benchmarks and portfolio optimization. *J Bank Financ* 2013;**37**:3515–28. https://doi.org/10.1016/j.jbankfin.2013.04.010
18. McKenzie M, Satchell S, Wongwachara W. Nonlinearity and smoothing in venture capital performance data. *J Empir Financ* 2012;**19**:782–95. https://doi.org/10.1016/j.jempfin.2012.08.004
19. Mezzetti A, Maréchal L, Percia David D,. *et al*. TechRank. *J Alternative Investments* 2024;**26**(3):57–83.https://doi.org/10.3905/jai.2023.1.202
20. Burguet F, Maréchal L, Mermoud A. The new risk and return of venture capital. *J Portfolio Manage* 2024;**50**:116–47.https://doi.org/10.3905/jpm.2024.1.611
21. ‘Crunchbase, Inc. ’, Historical Company Data. 2022. Crunchbase daily ∗.csv export, https://data.crunchbase.com/docs/daily-csv-export (data retrieved on April 2022).
22. Besten den ML. Crunchbase research: monitoring entrepreneurship research in the age of big data. 2021. http://dxdoiorg/102139/ssrn3724395 (12 May 2022, date last accessed).
23. Dalle JM, Besten den ML, Menon C. Using Crunchbase for economic and managerial research. 2017. https://doiorg/101787/18151965.
24. Hervé F, Schwienbacher A. Round-number bias in investment: Evidence from equity crowdfunding. *Finance* 2018;**39**(1):71–105. https://doi.org/10.3917/fina.391.0071
25. Alexy OT, Block JH, Sandner P,. *et al*. Social capital of venture capitalists and start-up funding. *Small Bus Econ* 2012;**39**:835–51. https://doi.org/10.1007/s11187-011-9337-4
26. Feurer M, Eggensperger K, Falkner S,. *et al*. Auto-Sklearn 2.0: Hands-free AutoML via meta-learning. 2021. https://arxivorg/abs/200704074 (20 April 2022, date last accessed).
27. Agrafiotis I, Nurse JRC, Goldsmith M,. *et al*. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J Cybersecur* 2018;**4**:1–15. https://doi.org/10.1093/cybsec/tyy006
28. Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). *Comput Secur* 2016;**57**:14–30. https://doi.org/10.1016/j.cose.2015.11.001
29. ‘National Institute of Standards and Technology, (NIST)’, Framework for improving critical infrastructure cybersecurity. 2018. https://nvlpubs.nist.gov/nistpubs/cswpnist.cswp.04162018.pdf (3 June 2022, date last accessed).
30. Ruan K. Introducing cybernomics: a unifying economic framework for measuring cyber risk. *Comput Secur* 2017;**65**:77–89. https://doi.org/10.1016/j.cose.2016.10.009
31. Hwang SY, Shin DJ, Kim JJ. Systematic review on identification and prediction of deep learning-based cyber security technology and convergence fields. *Symmetry* 2022;**14**:1–37.
32. Gordon LA, Loeb MP, Zhou L,. *et al*. Empirical evidence on disclosing cyber breaches in an 8-K report: Initial exploratory evidence. *J Account Public Policy* 2024;**46**:107226. https://doi.org/10.1016/j.jaccpubpol.2024.107226