Cyber Risk-Driven Innovation in the Modern Data Economy

Orlando Gomes[*], Roxana Mihet[†] and Kumar Rishabh[‡§]

February 29, 2024

Abstract

How and to what extent does cyber risk impact firms in the modern data economy? When firms face a high risk of losing their data and algorithms, this unequivocally leads to reduced knowledge stocks, decreased productivity, and slower overall economic growth. Notwithstanding, the empirical analysis pursued in this study suggests that cyber risk may also mitigate some of its own adverse effects as it ex-ante prompts digitally-savvy firms to pursue digital innovation that can enhance productivity in other domains. We observe increased innovation rates in response to higher cyber risk, driven primarily by data-intensive firms and by firms which intensively pursue in-house cyber security protection rather than third-party cyber security delegation. In a second stage, we develop a structural heterogeneous-firm growth model of the data economy to illustrate and explain the channels through which cyber risk exerts influence over firms' productivity, profits and growth.

Keywords: Data economy, cyber risk, growth, artificial intelligence, innovation.

JEL-Codes: D8, O3, O4, G3, L1, L2, M1.

[*]Lisbon Accounting and Business School, ISCAL. Contact: omgomes@iscal.ipl.pt

[†]Swiss Finance Institute at HEC Lausanne and CEPR. Contact: roxana.mihet@unil.ch

[‡]University of Lausanne and University of Basel. Contact: kumar.rishabh@unil.ch

[§]First version: January 31, 2023. This version: February 29, 2024. We are indebted to Chris Florackis, Christodoulos Louca, Roni Michaely, and Michael Weber for sharing their data on cyber-risk with us. We also thank Elliott Bertrand from Effixis for sharing data intelligence and Francesco Celentano for sharing public cyber-attacks data from Audit Analytics. We also thank our discussants, Fabrice Collard, Luca Sandrini, and Baozhong Yang for their helpful feedback, as well as participants at various conferences such as: EEA 2023, SFI Annual Days 2023, the Economics of ICT 2023, 4th Annual Boca-ECGI, ERMAS 2023, Toulose Digital Economics 2024, and WEIS 2024 for useful feedback. We are also grateful for insightful suggestions from Andreas Fuster, Tarun Ramadorai, Norman Schürhoff and Laura Veldkamp. Roxana Mihet acknowledges generous funding for this project from The Sandoz Family Foundation - Monique de Meuron Programme, as well as from UNIL's Dean's Office. All authors declare no conflicts of interest related to this project. All errors are our own. Corresponding author: roxana.mihet@unil.ch.

1 Motivation

The cost of business data breaches and theft can be significant and long-lasting. For firms, cybercrime can lead to financial losses, loss of sensitive information, lost productivity, reputation damage, legal consequences, and decreased customer trust. Cyberattacks can also disrupt business operations and result in costly downtime. Additionally, the resources spent on preventing and mitigating cybercrime could be put towards other investments that could foster economic growth. For societies, the cost of cybercrime goes beyond financial losses, and can range from compromised infrastructure, to national security issues, to missed economic opportunities. In the last 10 years in the United States, the monetary damage caused by reported cybercrime increased 12 fold from $ 581 million in 2012 to $ 6.9 billion in 2022 (ICCC).[1] As cybercrime is becoming costlier, more frequent and more aggressive over time, regulators are worried that it could harm U.S. companies' ability to remain leaders in innovation globally, thus undermining as well the pace of worldwide innovation.

In the first part of the paper, we quantify the impact of cybercrime risk on firm growth and innovation. We find that cybercrime attacks naturally result in lower stocks of knowledge, lost productivity and lower growth for all firms in the economy. But, with in-house cybersecurity protection, long-run sustained growth remains achievable even in the presence of cybercrime risk. The mechanism through which this occurs is that cybercrime risk ex-ante prompts firms to pursue digital innovation that enhances productivity in other domains. Cybercrime risk forces companies to improve their in-house security measures and systems, which can lead to new technology and products being developed. The need to protect against cyber-threats creates a demand for more secure software, hardware, and services, which leads to technological advancements and to sustained long-term growth. This positive externality is mainly driven by data-intensive firms, who benefit the most from protecting their data. The technology they develop for their own protection, combined with their data sophistication, helps them make even better predictions to create new products and improve the quality and diversity of their existing products.

We quantify empirically this potential positive externality by examining the impact

[1] While accurately estimating the total cost of cybercrime is difficult because the costs comprise not only of criminal revenue and direct losses, but also indirect losses and defense costs (Anderson et al. (2012), most recent reports suggest that global damages caused by cybercrime will surpass $8 trillion in 2023 and $10.5 trillion by 2025 (Cybersecurity Ventures 2022). To put it in perspective, only eighteen countries in the world had a GDP in 2022 larger than one trillion dollars.

of cybercrime risk on cybersecurity innovation and overall innovation. We first create a firm-year measure of cyber risk from 2007 to 2022 using the text-based NLP method of Florackis et al. (2023), which essentially compares the business description in a firm's 10K to the business description of a set of publicly data-breached firms. We use this measure to investigate whether companies that are highly exposed to cyber risk hedge themselves against this risk by innovating more. The novelty of our approach is to examine the endogenous response of firms subject to heterogeneous levels of cyber risk; and we find that firms do mitigate the negative effects of cyber risk by innovating more. Moreover, we examine multiple measures of innovation, such as patent counts, patent varieties, and patenting times. In current work, we are expending our analysis to delve deeper into firm boundaries and firm trademarks.

The direct analysis is complicated by the intertwined relationship where cyberrisk and innovation mutually influence each other, making it challenging to establish a clear cause-and-effect relationship. For example, firms that are more innovative might be more susceptible to cyberrisk to begin with. To address endogeneity concerns, we then employ an instrumental variables approach. Our instrument is the staggered adoption of Data Breach Notification Laws in the United States. These laws have been shown to increase firm risk related to data breaches (Boasiako and Keefe (2021); Liu and Ni (2023); Huang and Wang (2021)). Our strategy is to compare the innovation activities of firms located in early-treated states to those of firms located in late-treated states, taking into account the "forbidden comparison" mis-specification in two-way fixed effects diff-in-diff models, unveiled in Goodman-Bacon (2021) and solved by Borusyak et al. (2022).

Both our direct estimation and our staggered difference-in-difference method suggest that firms experience an increase in patenting activity, and an expansion in the diversity of the patent fields, in response to an increase in cybercrime risk, controlling for a multitude of firm-level characteristics. We also find that firms' profitability outcomes do not change with cybercrime risk because the risk is hedged by innovation. These results are driven by data-intensive digital firms which intensively develop in-house cybersecurity protection. This is because in digital data-intensive enterprises producing mostly digital goods, the IT department in charge of cyberprotection is also the R&D department in charge of product development. A concrete example is that in the pursuit of finding ways to securely store and transmit financial information over internet networks, Amazon used their own-built solution (Amazon's 9th most cited patent in the world) to offer the new "1-Click ordering" feature (Amazon's most cited patent).

Similar products have been developed by Apple, Uber, Alibaba's various platforms, such as AliExpress and Taobao, and Walmart which now offer streamlined checkout experiences, aiming to simplify the purchasing process for their customers, though not exactly identical to Amazon's 1-Click due to patent restrictions and each company's unique approach to improving the user purchasing experience.[2]

In the second part of the study, empirical findings serve as the background scenario to develop a theoretical framework aimed at formalizing the main mechanisms underlying the interaction between cyber risk and digital innovation, together with the individual and combined effects of these phenomena on economic growth. We build a heterogeneous-firm growth model of the data economy, in which data is information that helps firms optimize their business processes and is subject to cybercrime risk, meaning that it can be damaged and destroyed by cyber criminals. Firms are heterogeneous in their data sophistication levels and are allowed to protect themselves against cybercrime risk. Protection can occur either by developing in-house security solutions that are specifically tailored to the firms' needs and/or by delegating cyber-protection to third-party companies (i.e., in the context of the model, by purchasing security from the first set of firms, which develop their own protection solutions). Both types of firms solve profit maximization problems and they both benefit from fighting cyber risk: for the latter, the single benefit of purchasing protection consists in preserving data; for the former, in-house innovation signifies not only the preservation of data but also an innovation spillover effect that increases the potential quality of the produced goods.

The remainder of the paper proceeds as follows. Section 2 undertakes a short systematic review of the related literature. Section 3 sets the stage for the empirical analysis and enunciates and tests our main predictions. Section 4 addresses endogeneity concerns by exploiting the staggered implementation of Data Breach Notification Laws in the United States. Section 5 presents the growth model of the data economy with cybercrime risk and cyber-protection. Lastly, Section 6 concludes.

2 Literature review

Our project contributes to multiple strands of literature. First, it is associated with recent work on data as a main driver of economic growth. We extend the theoretical

[2]Apple's iTunes and App Store have a feature called "Buy with One Click", the ride-hailing service Uber introduced "Uber One Click", and Walmart, AliExpress and Taobao have all experimented with a "Fast Checkout" feature.

framework in Farboodi et al. (2019) and Farboodi and Veldkamp (2021) to include cybercrime in an growth model where data is a key input for prediction. In this literature, data is a valuable asset that helps firms reduce uncertainty about their associated production technique, making them approach a predetermined optimal benchmark. This class of models does not qualify growth as being endogenous: because lowering uncertainty about the best use of a given technique is a process subject to diminishing returns, in this scenario the economy evolves to a zero-growth long-term steady state.

The above interpretation collides with another related strand of thought, in which data has a different role, namely serving as an input in the production of ideas. In the context of endogenous growth theory, the relevance of data as an innovation device (i.e., as a decisive input in expanding the innovation frontier) was first highlighted by Jones and Tonetti (2020), who emphasized its key role as a vehicle for sustained growth. Data is a partially non-rival input whose generation emerges as a by-product of economic transactions. Its peculiar nature and its potential to assist in the creation of wealth has attracted much attention, namely in the context of endogenous growth models. A few relevant studies include Cong et al. (2021) and Cong et al. (2022), who explore models with consumer-generated data as a new factor for knowledge accumulation; Hou et al. (2022), who confront the possibility of sustained growth via data accumulation with the constraint associated with the economy's data storage capacity; Canayaz et al. (2022), who approach growth on the data economy by assessing the limiting role of data privacy laws over the acquisition, processing, and trade of consumer personal data.

The model to set forth in this paper is not an endogenous growth model, since data is not assumed as an input in the production of goods or an input in the innovation sector. It is fundamentally a prediction device. However, the possibility of innovation and growth is not excluded, because innovation emerges as a by-product of cyber security. Hence, when firms employ data they are reducing uncertainty, but they also become vulnerable to cyber incidents. This weakness can, in turn, become their strength, as the need to protect against cyber crime compels forms to innovate. As long as the need to protect exists, the incentive to innovate exists as well (at least for part of the firms in the market) and therefore sustained grwoth is a possibility in an environment in which data mainly serves the purpose of improving the accuracy in the use of the available production techniques.

Beyond theory, we also contribute to the empirical literature on the consequences of cybercrime on firm financial and economic outcomes. Florackis et al. (2023) develops a measure of corporate cyber risk for the period 2007-2018 for approximately 3100

U.S.-based publicly-listed firms and finds that this risk is priced in the stock market in the form of higher future returns. Such measure of cyber risk is employed throughout our empirical analysis to assess the link between cyber threats and the propensity to innovate.

Other cyber threat measures have been developed, as it is the case of Jamilov et al. (2021b), who uses quarterly earnings conference calls of listed firms to build a measure of cyber risk exposure and shows that this indicator predicts cyber attacks, affects stock returns and profits, and is priced in the equity option market. Kamiya et al. (2021), in turn, studies the financial performance of firms that are successfully cyber-attacked, as well as the ex-ante characteristics of those firms that are attacked. Both these studies show that cyberrisk is ex-ante positively correlated with firm size, growth opportunities (Tobin's Q), profitability (ROA) and expenditures of research and development (R&D), but R&D expenses are not correlated with the ex-post probability of a cyberattack. Moreover, those firms that are successfully attacked experience negative cumulative abnormal returns around the attack, and attacks have a significant negative long-term impact on sales growth, customer confidence, and in operating performance. Relative to these studies, we examine the impact of cybercrime risk on firms' innovation activities, looking particularly at their issuance of patents and - in ongoing work - trademarks.

On the empirical front, our primary aim is to understand the nexus between cybercrime risk and cyber security innovation, and their influence on a firm's overall innovation. Lattanzio and Ma (2023) document that firms exposed to cyber threats file for simpler patents to accelerate their innovation cycle. This strategic adjustment is costly, causing firms' R&D activities to decline considerably. Distinct from Lattanzio and Ma (2023), we examine more closely the channels through which this innovation cycle occurs. We find that it is driven by data intensive firms, as measured by our unique method that uses computational linguistics to measure data intensity based on text similarity between the 10Ks of listed firms relative to a control group of digital AI-intensive firms. In particular, these data-intensive firms tend to file more cyber security patents which are then later useful for other non-cyber security related patents. Moreover, we document that only in-house cyber security innovation sustains this innovation cycle. Firms that delegate cyber security to a third-party do not benefit from the same positive externalities caused by in-house cyber security protection.

3 Empirical Analysis

The starting point of the pursued empirical analysis consists in inquiring to which extent firms can effectively address the negative consequences of cyber risk through innovation. Specifically, we investigate whether firms facing higher cyber risk evidence higher levels of innovation. To quantify the mechanisms discussed in our paper, we analyze whether firms with considerable associated cyber risk engage in innovative practices related to cyber security. Additionally, we explore whether these firms exhibit higher overall innovation levels, encompassing both cyber security and non-cyber security domains. We further test whether the data intensive firms are the main drivers of our results.

3.1 Data

Answering our research question requires two elements. First, a measure of firm level cybercrime risk. Second, a measure of innovation at the firm level.

We source our measure of cybercrime risk for US-based publicly listed firms from Florackis et al. (2023). The authors have designed a cyber security risk score based on a textual analysis of the annual 10-K filings of these companies. For any given year, a firm's risk measure is derived from the similarity between the language used to detail *cyber risk-factors* in its current-year 10-K filings and the *previous-year* 10-K filings of a chosen 'training' set of firms. The firms in this training set are those that endured actual cyber attacks in the same year. The assumption is that firms that have fallen prey to actual cyber attacks likely had existing vulnerabilities, which would have been reflected in their risk disclosures in the previous year. As such, if a firm's language in its risk-factor disclosures strongly resembles the previous-year risk disclosures of firms that were indeed attacked, it is inferred to bear a high cyber security risk. The similarity score, which also serves as the cyber risk score, ranges from zero to one, with a higher score indicating a greater cyber risk.[3] These cyber risk scores are available for the period from 2007 to 2018. Accordingly, we calculate all other remaining variables within this same period.

[3]We believe these are good measures of firm cyber risk because US firms are required by law to report data breaches in all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands, and therefore they are highly likely to be forthcoming about their cyber risk and risk mitigation in their 10-Ks (Murciano-Goroff (n.d.)). Moreover, we are confident in the validity of this measure because, according to the undertaken calculations, it correlates highly (86%) with the cyber risk measure based on conference calls from Jamilov et al. (2021a).

We capture innovation in various complementary ways. The first measure we use is the knowledge capital accumulation calculated by Ewens et al. (2020). Knowledge capital is the stock of research and development (R&D) expenditure net of the knowledge capital depreciation. Knowledge asset can also be thought of as an input to innovation, rather than output, as it represents expenditure on producing innovation. Our next set of measures explicitly capture innovation output.

Firms' patent activity represent their innovation output. Following the literature on innovation, we count patents filed by the firms by taking into account their scientific and economic value (Kogan et al., 2017; Aghion et al., 2013; Howell, 2017). In our first patent measure, we count number of patents filed by weighing it with the number of forward citations they receive. The idea is that the more scientifically important a patent is, the more citations it receives (Hall et al., 2005; Kogan et al., 2017). Following the best practice in the literature, we adjust the count for the truncation bias. As the citations occur over time, a simple counting of cites underestimates the importance of the patents that were issued towards the end of our sample period (Lerner and Seru, 2022; Dass et al., 2017; Hall et al., 2001). We correct for that using the well-established methodology proposed by Hall et al. (2001).

We also calculate value-weighted count of number of patents filed. We do so by weighing each patent by the economic value it creates. The economic value of a patent is the dollar amount of wealth generated for the patenting firm's shareholders, calculated from the stock market response to the news about the patent award. We scale the patent value by the firm's total assets, following Kogan et al. (2017).

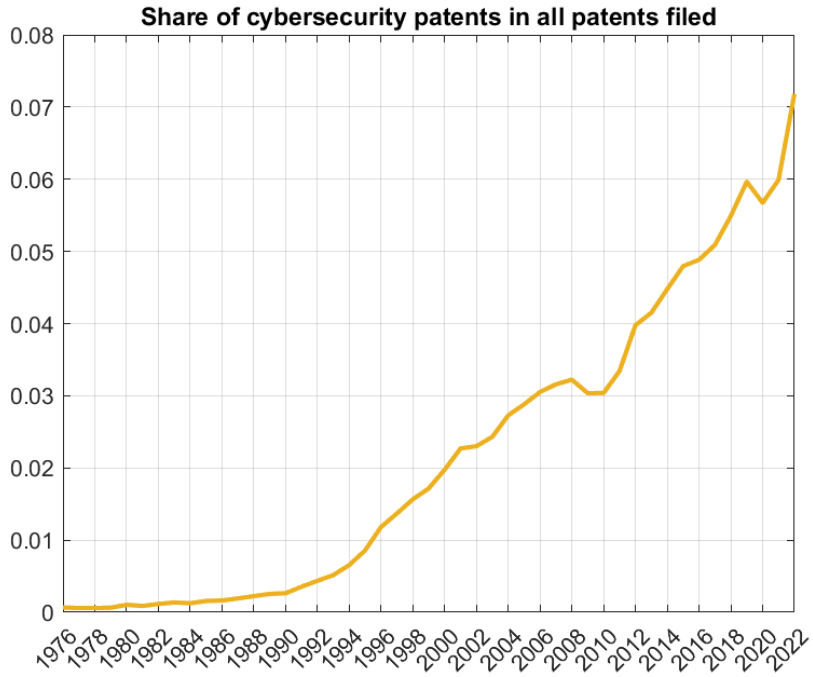
In an additional analysis, we examine whether firms exposed to more risks expand their areas of innovation. To do that, we extract the Cooperative Patent Classification (CPC) code for each filed patent. We then count the number of unique 'fields' in which a firm files patents in a year. We define number of fields at different level of coarseness. A CPC code consists of five hierarchical parts: section, class, sub-class, group, and sub-group. Section is the highest level in hierarchy, and the most aggregative level, followed by class, subclass, and so on. For our purpose, we define patent fields at three alternative levels: section, class, and sub-class. We do not differentiate patents along the group or subgroup levels because we want to make sure that we are counting patent fields that are somewhat distinct from each other.

All our patent data is from the publicly available database maintained by the authors of Kogan et al. (2017).

We measure cybersecurity innovation using the citation-weighted and value-weighted

count of cybersecurity patents a firm files within a year. A patent is classified as a cybersecurity patent if the USPTO assigns it CPC codes associated with cybersecurity. For instance, CPC code G06F21/ is titled "Security arrangements for protecting computers, components thereof, programs or data against unauthorised activity". Our cybersecurity patent measure indicates a consistent growth in cybersecurity innovation over time, currently accounting for approximately seven percent of all patent filings (as depicted in Figure 1).

Figure 1: Cybersecurity innovation



To identify data-intensive firms, we create a measure grounded on two fundamental premises. First, we propose that firms involved in the creation of AI technology are, by nature, data-intensive. Second, we posit that any firm, including those not directly engaged in AI development, can be considered data-intensive if the language used to describe its business mirrors that of AI-creating firms. In accordance with these premises, our measure is crafted in two steps. For the initial step, we utilize a newly published dataset by the USPTO, a product of their internal research, which classifies AI patents within the entire spectrum of patents filed at the USPTO Giczy et al. (2022). This helps us identify those US public firms that have submitted AI patent applications. In the second step, we employ a dataset curated by Hoberg and Phillips, which quantifies

the textual similarity in the Business Description between any two firms (Hoberg and Phillips, 2016). The underlying principle here is that data-intensive firms are likely to portray their businesses in a similar light. Therefore, a firm not holding an AI patent is also considered data-intensive if its business description more closely aligns with those firms possessing AI patents.

We obtain firm level financial information from the merged CRSP-Compustat database. We calculate various financial variables and ratios to use them as control variables in our baseline regressions. Specifically, we use the following variables as controls: log of total assets, tobin's Q, asset tangibility, book-to-market ratio, cash-to-asset ratio, leverage, and return on assets. We winsorize all the variables at 0.5% on both sides of the distribution.

Table 1 presents summary statistics on our cyber risk and innovation measures. We see that more than a quarter of the firms do not face cyber risk. Further, as is well-known innovation activity is quite skewed. For instance, more than 50 percent of firm-years do not record any positive knowledge capital accumulation or any patent activity.

Table 1: Summary statistics on cyber-risk score and innovation variables

	N	mean	sd	p10	p25	p50	p75	p90	p99
Cyber-risk score	44972	0.2	0.2	0	0	0.3	0.4	0.5	0.6
Log(Knowledge stock)	41479	1.6	2.2	0	0	0	3.4	5.0	8.0
Log(R&D expenditure)	44972	1.3	1.9	0	0	0	2.6	4.2	7.2
Patents filed: simple count	44972	9.2	49.9	0	0	0	0	8.0	291.0
Patents filed: citation-weighted count	44972	18.3	100.4	0	0	0	0	15.3	549.4
Patents filed: value-weighted count	44881	0.05	0.20	0	0	0	0	0.11	1.17
Number of patent sections	10616	3.3	2.0	1	2	3	4	6	9
Number of patent classes	10616	7.5	10.3	1	2	4	8	17	57
Number of patent subclasses	10616	14.1	25.0	1	3	6	14	31	145

N refers to the total number of firm-year. p10-p99 refer to the 10th to 99th percentile values. Cyber risk score lies between zero and one, with higher values indicating higher risk. Cyber risk score measure is obtained from Florackis et al. (2023). Knowledge stock is based on the estimates of knowledge stock net of knowledge depreciation from Ewens et al. (2020). Simple patent count refers to number of patents filed by the firm in a year. Citation-weighted patent count weighs each patent with the forward citation the patent receives, adjusting for the filing vintage. Value-weighted patent count is the sum of stock market value generated over all the patents filed by a firm in a year, scaled by total assets. Number of patent sections refers to the number of unique CPC sections associated with all the patent the firm files in a year. Similar explanation applies to patent classes, and subclasses, respectively.

3.2 Empirical strategy

We conduct regression analysis to uncover the relationship between cyber risk and innovation. We rely on two aspects of our regression specification to identify the causal relation between cyber risk and innovation. First, we regress innovation measures on the lagged value of cyber risk score. Doing so addresses the simultaneity concerns. Second, we include firm fixed effects to absorb time invariant characteristics of firms that might affect this relationship. Moreover, we include year fixed effects to absorb shocks occurring over time and that are common across firms. Finally, we control for various financial factors.

As visible from Table 1, our innovation variables have a right skew and contain a high share of zeros. Therefore, applying ordinary least squares (OLS) estimation in a regression of the patent counts might result in inefficient parameter estimates. One possible solution could be using OLS estimation after a log transformation of our patent count variables. However, given the large number of zeros, a log transformation excludes a substantial number of observations when estimating log-linear regressions. More importantly, log-linear regressions may even produce inconsistent estimates of the parameters (Silva and Tenreyro, 2011). Alternatively, we could log transform after adding 1 to each patent count, or apply inverse hyperbolic sine transformation. These transformations would retain zeros, however, they may also produce inconsistent estimates. Moreover, they may even have the opposite sign of the true relationship, as shown by Cohn et al. (2022).[4]

Econometricians recommend the Poisson model to explicitly take into account many zeros and the right skew of the dependent variables. Because, in such a setting too, a Poisson model produces consistent estimators without requiring any assumptions about higher order model error moments (Cohn et al., 2022). In addition, and importantly for us, Poisson regression allows for separable group fixed effects (Correia et al., 2020; Cohn et al., 2022). Moreover, even though the Poisson model is generally considered to be useful for count data (such as patents), actually, it is valid even when the dependent variable is continuous with a non-negative domain (such as knowledge asset) (Silva and Tenreyro, 2011; Wooldridge, 1999).[5]

To study the relationship between the lagged value of cyber risk score (crscore_{it-1})

[4]Though, less fatal than other flaws the parameter estimates are also hard to interpret after the transformations (Cohn et al., 2022; Silva and Tenreyro, 2006).

[5]Well-known works employing Poisson regression with patent data include Azoulay et al. (2019); Aghion et al. (2013); Amore et al. (2013); Blundell et al. (1999); Hausman et al. (1984).

and innovation measure (innovation_{it}) we fit the following conditional expectation of an innovation measure that follows a Poisson distribution:

$$\mathbb{E}[\text{innovation}_{it}|\text{crscore}_{it-1}, \mathbf{x}_{it-1}, \eta_i, \tau_t] = \exp\left(\beta_c \text{crscore}_{it-1} + \beta \mathbf{x}_{it-1} + \eta_i + \tau_t\right) \quad (1)$$

where crscore_{it-1} is the lagged value of cyber-risk score, $\mathbf{x}_{it-1}$ are *lagged* control variables, including size (log of total assets), Tobin's Q, asset tangibility, book-to-market ratio, cash-to-asset ratio, leverage, and return on assets. η_i is the firm fixed effect, and τ_t is the year fixed effect.

We perform Poisson pseudo-maximum likelihood estimation to estimate the parameters of the model in (1).

We also study whether cyber risk score affects the *R&D productivity*. To do that, we follow Aghion et al. (2013), and in some specifications of (1) include *R&D stock* as a right hand side variable. In such specifications, the coefficient β_c tells us whether firms with higher score innovate more per dollar of R&D stock. In specifications, where *R&D stock* is not included as a control variable, β_c contains the effect of R&D productivity and additional effect of higher cyber risk on innovation.

Finally, we cluster standard errors at the firm level, to take into account the possibility of autocorrelation and hetereskedasticity in the error terms. Clustered standard errors are additionally useful because they are also robust to 'overdispersion' (and 'underdispersion') issues countered in Poisson regression (Cohn et al., 2022; Wooldridge, 1999).

3.3 Baseline results

In what follows, we report the results from our preferred Poisson estimation. We also report estimates from OLS regression of our innovation measures.[6]

Table 2 presents the results of regressing knowledge capital and R&D stock on lagged cyber-risk score. We find that firms accumulate more knowledge capital and R&D stock in response to a rise in cyber risk. Although, in the regression of knowledge capital, the Poisson model does not give a significant coefficient for cyber risk at the conventional 10% significance level, the value is quite close. Moreover, the results are also confirmed by the regression of R&D stock, which shows a significant rise. The increase is also economically meaningful. For instance, one standard deviation change

[6]Although, fully recognizing that this might not be the correct model specification.

in cyber risk would lead to an increase in R&D by about 3% [$= 0.22(e^{0.124} - 1)$], keeping everything else the same.

How do firms respond with their patenting output when they face a higher cyber risk? Do they file more patents because they accumulate more R&D stock, or do they also respond by increasing their R&D productivity? To test that, we regress patent-count variables on lagged cyber-risk in Table 3 and Table 4. The first two columns of both tables exclude R&D as a control variable. Therefore, these specifications test the change in firm's innovation output to cyber risk. The change includes the effect of cyber risk on innovation input, as well as its effect on the R&D productivity. In columns (3) and (4) we also include the stock of R&D capital as an explanatory variable. Therefore, the coefficient on cyber-risk score gives us the estimate of how in response to an increase in cyber risk, a firm's patent count changes keeping its innovation input (R&D capital) unchanged.

Table 3 presents the regression results with citation-weighted patent count as the dependent variable. The first observation we make is that in all the specification in the table, the coefficient on Cyber-risk score is positive, indicating that firms patent more in response to a cyber-risk shock. From our Poisson estimate in column (2), we can quantify the effect. A one standard deviation increase in cyber risk in a year leads the firm to file 5% [$= 0.22(e^{0.201} - 1)$] more patents the next year. We observe from column (4) that firms file more patents per dollar of R&D stock. We estimate that in response to a one standard-deviation shock in cyber risk, firm's R&D productivity rises by about 4.2%.

We arrive at a similar conclusion when we use value-weighted patent count in Table 4. A one standard-deviation shock in cyber risk leads to the firm filing about 7% more patents in value-weighted terms (column 2). Out of this increase, about 6% is due to the increase in R&D productivity (column 4).

3.4 Cyber risk and cyber security innovation

To thoroughly investigate the mechanisms underpinning the relationship between cyber security and innovation, we proceed by inquiring about whether firms exposed to heightened cyber risk are more likely to increase their focus on cyber security innovation. Subsequently, we explore if an uptick in cyber security innovation could stimulate a broader surge in overall innovation. In the ensuing regression tables, we restrict our focus to the pertinent coefficient estimates, suppressing those associated with the

Table 2: Regression of knowledge stock and R&D stock

	Knowledge stock		R&D stock	
	OLS	Poisson	OLS	Poisson
	(1)	(2)	(3)	(4)
Cyber-risk score	21.38**	0.0868	9.755**	0.124*
	(9.223)	(0.0542)	(4.468)	(0.0659)
ln(Asset)	60.23***	0.486***	32.03***	0.551***
	(9.959)	(0.0381)	(5.202)	(0.0339)
Tobin's Q	2.894**	0.0300***	2.557***	0.0537***
	(1.359)	(0.00622)	(0.697)	(0.00773)
Tangibility	-2.051	0.484*	-9.190	0.286
	(30.26)	(0.253)	(13.67)	(0.271)
Book-to-market	-0.781	-0.0224**	0.319	0.00190
	(1.013)	(0.0109)	(1.018)	(0.0413)
Cash-to-asset	-45.29***	-0.169*	-24.91***	-0.195*
	(16.80)	(0.0895)	(6.908)	(0.106)
Leverage	-5.477	-0.150*	-3.998	-0.212**
	(15.01)	(0.0798)	(6.407)	(0.0841)
ROA	-45.97***	-0.216***	-18.87***	0.00708
	(11.22)	(0.0716)	(5.475)	(0.0749)
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
N	31601	14921	34592	15038

$^{*}p < 0.10,^{**}p < 0.05,^{***}p < 0.01$. Standard errors are in parentheses. Standard errors are clustered at the firm level. N refers to the total number of firm-year. Cyber score, and control variables are lagged by one year. Cyber-risk score measure is obtained from Florackis et al. (2023). Knowledge stock is based on the estimates of knowledge stock net of knowledge depreciation from Ewens et al. (2020). Other control variables are computed using WRDS CRSP-Compustat merged data. Tobin's Q is defined as Total assets (at) minus common equity (ceq) plus market value of equity (prcc_f × csho), as a ratio of total assets (at). ROA is defined as operating income before depreciation (oibdp) to total assets (at). Tangibility is defined as total property, plant and equipment (ppent) scaled by total assets (at). Leverage is long-term debt (dltt) plus debt in current liabilities (dlc), as a ratio of total assets (at). Book-to-market ratio is book value of common equity (ceq) divided by the market value of common equity (prcc_f × csho). Cash-to-asset is the ratio of cash and short-term investments (che) to total assets (at).

Table 3: Regression of citation-weighted patent count

	Citation-weighted patent count			
	OLS	Poisson	OLS	Poisson
	(1)	(2)	(3)	(4)
Cyber-risk score	4.060*	0.201**	3.784*	0.176*
	(2.135)	(0.101)	(2.138)	(0.0994)
ln(Asset)	2.064**	0.141***	1.190*	0.0352
	(0.824)	(0.0493)	(0.716)	(0.0516)
Tobin's Q	0.282	0.0159	0.268	0.0139
	(0.283)	(0.0153)	(0.282)	(0.0154)
Tangibility	3.032	0.0758	2.834	-0.0657
	(5.990)	(0.559)	(5.979)	(0.538)
Book-to-market	-0.00283	0.0186	0.0392	0.0233
	(0.247)	(0.0516)	(0.248)	(0.0516)
Cash-to-asset	-3.186	-0.00373	-2.717	0.0565
	(2.590)	(0.150)	(2.570)	(0.148)
Leverage	-4.420*	-0.163	-4.257*	-0.107
	(2.297)	(0.189)	(2.295)	(0.191)
ROA	-0.371	0.105	0.603	0.151
	(1.295)	(0.184)	(1.289)	(0.181)
ln(R&D stock)			2.978***	0.190***
			(0.757)	(0.0441)
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
N	34592	12900	34592	12900

$^{*}p < 0.10,^{**}p < 0.05,^{***}p < 0.01$. Standard errors are in parentheses. Standard errors are clustered at the firm level. Cyber score, and control variables are lagged by one year. Cyber-risk score measure is obtained from Florackis et al. (2023). Citation-weighted patent count weighs each patent with the forward citation the patent receives, adjusting for the filing vintage. For the description of control variables, see notes for Table 2.

Table 4: Regression of value-weighted patent count

	Value-weighted patent count			
	OLS	Poisson	OLS	Poisson
	(1)	(2)	(3)	(4)
Cyber-risk score	0.0182***	0.277**	0.0186***	0.238**
	(0.00703)	(0.122)	(0.00699)	(0.116)
ln(Asset)	-0.0266***	-0.301***	-0.0252***	-0.413***
	(0.00449)	(0.0489)	(0.00406)	(0.0568)
Tobin's Q	0.00197	0.00296	0.00199	-0.00128
	(0.00184)	(0.00836)	(0.00183)	(0.00826)
Tangibility	0.0171	0.351	0.0173	0.135
	(0.0211)	(0.455)	(0.0211)	(0.456)
Book-to-market	0.00190**	-0.0961	0.00184*	-0.0955
	(0.000943)	(0.0644)	(0.000941)	(0.0639)
Cash-to-asset	0.0466***	0.468***	0.0459***	0.501***
	(0.0161)	(0.160)	(0.0163)	(0.155)
Leverage	0.0162	-0.00786	0.0160	0.0386
	(0.0116)	(0.111)	(0.0115)	(0.107)
ROA	0.00119	0.0900	-0.000269	0.202**
	(0.0113)	(0.0878)	(0.0111)	(0.0879)
ln(R&D stock)			-0.00446	0.178***
			(0.00449)	(0.0530)
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
N	34579	12896	34579	12896

$^{*}p < 0.10,^{**}p < 0.05,^{***}p < 0.01$. Standard errors are in parentheses. Standard errors are clustered at the firm level. N refers to the total number of firm-year. Cyber-risk score, and control variables are lagged by one year. Cyber risk score measure is obtained from Florackis et al. (2023). Value-weighted patent count is the sum of stock market value generated over all the patents filed by a firm in a year, scaled by total assets. For the description of control variables, see notes for Table 2.

controls. Further, we now work exclusively with our preferred Poisson model.

Table 5 displays the regression of the number of filed cyber security patents against the lagged cyber risk, across different specifications. All regression models incorporate the controls used in previous analyses, log of R&D stock, and year fixed effects. Industry fixed effects are included in columns (1) through (4), while firm fixed effects are applied in specifications (5) and (6). The industry fixed effects are used in the initial specifications due to the fact that a relatively small number of firms file cyber security patents. This leads to a reduced number of observations if we apply firm fixed effects, which complicates the task of obtaining precise estimates. Within the first four specifications, we alternate between the exclusion and inclusion of the lagged count of both cyber security and overall patents.

Our analysis indicates that an increase in cyber risk prompts firms to file a greater number of cybersecurity patents. This positive effect is still evident in the most restrictive specification featuring firm fixed effects. However, due to the limited number of observations, we cannot assert our conclusions with complete confidence.

Table 5: Regression of cyber security innovation

	Cit-wtd CS patent #		Val-wtd CS patent #		Cit-wtd CS patent #	Val-wtd CS patent #
	(1)	(2)	(3)	(4)	(5)	(6)
L.Cyber risk	1.155***	0.664***	1.780***	1.170***	0.0921	0.0108
	(0.352)	(0.246)	(0.400)	(0.401)	(0.238)	(0.286)
L.# cit-wtd CS patent	No	Yes	No	No	No	No
L.# val-wtd CS patent	No	No	No	Yes	No	No
L.# cit-wtd patent	No	Yes	No	No	No	No
L.# val-wtd patent	No	No	No	Yes	No	No
Size + other controls	Yes	Yes	Yes	Yes	Yes	Yes
NAICS-3 FE	Yes	Yes	Yes	Yes	No	No
Firm FE	No	No	No	No	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
N	29283	29283	29273	29273	3502	3501

In order to examine the next segment of the loop, we investigate whether firms with a higher degree of innovation in cyber security also exhibit a greater level of overall innovation. We undertake regression analyses where we regress citation-weighted and value-weighted patent counts against both the lagged counts of cyber security patent filings and the lagged cyber risk scores (as presented in Table 6).

Columns (1) and (2) in Table 6 mirror our previous baseline findings. In the subsequent models, we also investigate the effect of the lagged counts of cybersecurity patents. We ascertain that an increase in cybersecurity patents leads to an overall surge

Table 6: Regression of counts of patent filed

	# Cit-wtd patent	# Val-wtd patent	# Cit-wtd patent		# Val-wtd patent	
	(1)	(2)	(3)	(4)	(5)	(6)
L.Cyber risk	0.199**	0.276**	0.0764	0.0716	0.220**	0.233**
	(0.101)	(0.122)	(0.0728)	(0.0736)	(0.0991)	(0.0984)
L.# cit-wtd CS patent			0.00286**	0.00135*		
			(0.00114)	(0.000802)		
L.# val-wtd CS patent					2.487***	1.607***
					(0.554)	(0.591)
# cit-wtd CS patent	No	No	No	Yes	No	No
# val-wtd CS patent	No	No	No	No	No	Yes
L.# cit-wtd patent	No	No	Yes	Yes	No	No
L.# val-wtd patent	No	No	No	No	Yes	Yes
Size + other controls	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
N	12900	12896	12900	12900	12896	12896

in innovation, as reflected in both measures of innovation. To refine our results, we also account for the contemporaneous counts of cybersecurity patents in specifications (4) and (6). Our results maintain their significance and positive orientation. This suggests that, even when the number of cybersecurity patents is held constant, there is an increase in the total number of patents when firms engage in cybersecurity innovation. This implies that firms also augment their portfolio of non-cybersecurity patents in response to cybersecurity innovation.

3.5 Data intensive firms and their response to cyber security risk

Next, we study how the above dynamics differ between the data-intensive and non-data intensive firms. Our model posits a feedback loop for the data economy, i.e. an economy reliant on the data that is subject to the risk of being stolen. We therefore, expect this mechanism to apply on data-intensive firms and not on the non-data-intensive firms.

We construct a dummy variable that takes value 1 if the firm is identified as a data intensive firm by our earlier described method. We then run the regressions similarly to those in the previous section, however now we interact the lagged cybersecurity score with the dummy on data intensity. The results are presented in Table 7.

We find that even though the data intensive firms account only for a minority of the observations (roughly 40%), our baseline results are driven by them. Indeed, the regressions show that cyber risk score has even sometimes negative effects on innovation in the non-data intensive firms, although, the results are never significant.

Table 7: Regression with data intensity

	Cit-wtd patent #	Val-wtd patent #	Cit-wtd patent #		Val-wtd patent #	
	(1)	(2)	(3)	(4)	(5)	(6)
L.Cyber risk*(data int =0)	-0.0872	0.186	-0.0607	-0.0463	0.215	0.260
	(0.156)	(0.191)	(0.109)	(0.111)	(0.157)	(0.162)
L.Cyber risk*(data int = 1)	0.289**	0.293**	0.121	0.110	0.221**	0.228**
	(0.115)	(0.126)	(0.0802)	(0.0807)	(0.104)	(0.103)
L.# cit-wtd CS patent			0.00281**	0.00131		
			(0.00114)	(0.000804)		
L.# val-wtd CS patent					2.487***	1.611***
					(0.554)	(0.590)
# cit-wtd CS patent	No	No	No	Yes	No	No
# val-wtd CS patent	No	No	No	No	No	Yes
L.# cit-wtd patent	No	No	Yes	Yes	No	No
L.# val-wtd patent	No	No	No	No	Yes	Yes
Size + other controls	Yes	Yes	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
N	12900	12896	12900	12900	12896	12896

3.6 Cyber risk and patent fields

Do firms broaden the fields in which they innovate in response to the cyber risk? To answer that, we regress the number of patent fields in a firm's patent filings on cyber risk scores (Table 8). We use different definitions of patent fields representing various levels of aggregation in CPC codes. Patent sections are at the top level, with different sections representing very distinct areas. Patent classes have smaller distinction across them, and so on.

We find that while point estimates are positive, they are not significant for section count or class count. For subclasses, there is a positive and significant effect of cyber risk when we estimate an OLS model. However, we cannot estimate it precisely with Poisson regression. Quantitatively, the change in number of subclasses in response to a rise in cyber risk is positive and non-negligible. A one standard deviation shock in cyber risk leads to a 0.4% increase in patent fields when we define fields in terms of the count of patent subclasses.

Overall, we find some evidence that firms expand the areas of innovation in response to cyber risk, even though we are reluctant to place a lot of confidence in this finding.

Table 8: Regression of patent-field count

	Count patent sections		Count patent classes		Count patent sub-classes	
	OLS	Poisson	OLS	Poisson	OLS	Poisson
	(1)	(2)	(3)	(4)	(5)	(6)
Cyber-risk score	0.0566	0.0106	0.583	0.00726	1.958**	0.0193
	(0.116)	(0.0338)	(0.424)	(0.0484)	(0.960)	(0.0521)
ln(Asset)	0.154***	0.0508***	0.839***	0.122***	2.086***	0.159***
	(0.0502)	(0.0168)	(0.265)	(0.0351)	(0.735)	(0.0468)
Tobin's Q	0.0118	0.00437	0.0133	0.00454	0.0365	0.00730
	(0.00875)	(0.00318)	(0.0299)	(0.00543)	(0.0732)	(0.00690)
Tangibility	-0.0134	0.00267	1.837	0.250	5.774	0.402
	(0.345)	(0.107)	(1.622)	(0.215)	(4.662)	(0.315)
Book-to-market	0.0162	0.00482	0.124	0.00926	0.378	0.0105
	(0.0426)	(0.0149)	(0.165)	(0.0241)	(0.418)	(0.0283)
Cash-to-asset	0.0686	0.0257	0.626	0.0911	1.026	0.0684
	(0.136)	(0.0469)	(0.443)	(0.0709)	(1.086)	(0.0851)
Leverage	-0.183	-0.0609	-0.254	-0.0581	-0.535	-0.0729
	(0.126)	(0.0438)	(0.401)	(0.0720)	(0.886)	(0.0876)
ROA	-0.00596	0.0117	-0.478	-0.000475	-1.462*	-0.00603
	(0.0870)	(0.0324)	(0.315)	(0.0519)	(0.798)	(0.0652)
ln(R&D stock)	0.0946**	0.0282**	0.195	0.0426*	0.160	0.0402
	(0.0373)	(0.0124)	(0.144)	(0.0230)	(0.364)	(0.0296)
Firm FE	Yes	Yes	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
N	8641	8641	8641	8641	8641	8641

$^{*}p < 0.10,^{**}p < 0.05,^{***}p < 0.01$. Standard errors are in parentheses. Standard errors are clustered at the firm level. N refers to the total number of firm-year. Cyber-risk score, and control variables are lagged by one year. Cyber risk score measure is obtained from Florackis et al. (2023). Number of patent sections refers to the number of unique CPC sections associated with all the patent the firm files in a year. Similar explanation applies to patent classes, and subclasses, respectively. For the description of control variables, see notes for Table 2.

3.7 Cyber risk and financial variables

Does a rise in cyber risk affect a firm's profitability? Cyber risk can reduce a firm's profitability by diverting its resources towards cyber protection measures. It might even go up if the higher innovation in response to cyber risk creates new profitable opportunities. However, the two forces might counteract each other as well.

Table 9 presents results of a set of regressions on different financial variables. The first column regresses return on assets (ROA) on lagged cyber risk measure and other controls. We find no negative effect of cyber risk on profitability, indicating that innovation helps firms to hedge their profits against cyber risk.

Table 9: Regression of financial variables

	ROA	Tobin's q	Book-to-market	Leverage
	(1)	(2)	(3)	(4)
Cyber-risk score	0.00885	0.0709	-0.0161	-0.00787
	(0.00851)	(0.0621)	(0.0372)	(0.00813)
ln(Asset)	0.0200***	-0.403***	0.232***	0.0366***
	(0.00543)	(0.0351)	(0.0184)	(0.00403)
Tobin's Q	0.0152***		-0.0360***	-0.00217
	(0.00251)		(0.00401)	(0.00179)
Tangibility	-0.0905***	-0.326*	0.282**	0.0792***
	(0.0312)	(0.184)	(0.113)	(0.0278)
Book-to-market	-0.0233***	-0.167***		-0.0180***
	(0.00282)	(0.0177)		(0.00287)
Cash-to-asset	-0.126***	0.493***	-0.116**	-0.108***
	(0.0208)	(0.150)	(0.0525)	(0.0162)
Leverage	-0.0107	0.284**	-0.618***	
	(0.0192)	(0.124)	(0.0574)	
ln(R&D stock)	-0.0245***	0.0482	-0.0270*	0.000962
	(0.00496)	(0.0311)	(0.0138)	(0.00445)
ROA		0.0187	-0.0782*	-0.0819***
		(0.121)	(0.0417)	(0.0138)
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
N	34591	34564	34564	34577

$^{*}p < 0.10,^{**}p < 0.05,^{***}p < 0.01$. Standard errors are in parentheses. Standard errors are clustered at the firm level. N refers to the total number of firm-year. Cyber-risk score, and control variables are lagged by one year. Cyber risk score measure is obtained from Florackis et al. (2023). ROA stands for return on assets. All estimations are based on OLS regression. For the description of variables, see notes for Table 2.

In a similar regression given in columns (2)-(4), we find no significant effect of cyber-risk shock on a firm's Tobin's Q, Book-to-market ratio, and Leverage.

3.8 General innovation and cyber risk

Our model suggests that a firm's reaction to cyber risk extends to broader innovation, beyond just cyber security innovation. We explore this by examining how a firm's non-cyber security innovation is affected by cyber risk. We analyze this relationship by regressing the non-cyber security patents of firms against their lagged cyber risk. Here, non-cyber security patents are described as those distinct from the set of cyber security patents identified earlier.

Our findings, presented in Table 10, indicate that firms increase their non-cyber security innovation by approximately eight percent in response to a one standard deviation (s.d.) increase in cyber risk (Column 1). When evaluating the impact in terms of value-weighted patent count, we observe a positive effect, with a one s.d. increase in cyber risk contributing to a four percent rise in non-cyber security innovation, although this effect is not statistically significant (Column 2).

Moreover, we notice that advancements in cyber security innovation (lagged cyber security patent counts) are associated with heightened non-cyber security innovation, regardless of the regression specification employed.

3.9 In-house cyber security innovation and cyber risk

We hypothesize that the innovation response to cyber risk is more pronounced for firms that undertake *in-house* cyber security innovation. This assertion stems from the notion that firms with *in-house* cyber security innovation are positioned to realize the benefits of the externality of innovation in response to cyber risks. To identify firms that develop cyber security *in-house*, we examine the backward citations of the public firms' patents. Backward citations refer to the citations a patent makes to preceding patents, which serve as references or foundational works for the current patent.

We sourced the dataset on backward patent citations from the USPTO, and for each patent by the firms in our sample, we ascertain (i) whether the patent they cite is a cyber security patent, and (ii) whether the cited patent belongs to the firm itself. Firms that cite their *own* cyber security patents are likely employing their own cyber security technology in other innovative areas. Thus, we designate a firm that cites its own cyber security patent in any of its patents as an in-house cyber security firm. Similarly, we designate a firm as an in-house firm by a narrow measure which cites its own cyber security patent in its *non-cyber security* patent. These designations remain unchanged across years for a given firm.

Table 10: Regression of non-cybersecurity patent count

	Citation-weighted count (1)	Value-weighted count (2)
Cyberrisk score	0.248**	0.142
	(0.111)	(0.109)
Cit-wtd CS patent	Yes	No
Val-wtd CS patent	No	Yes
Size + other controls	Yes	Yes
Firm FE	Yes	Yes
Year FE	Yes	Yes
N	14122	13704

$^{*}p < 0.10,^{**}p < 0.05,^{***}p < 0.01$. The coefficient estimates are derived from the Poisson pseudo-maximum likelihood estimation. Standard errors are in parentheses. Standard errors are clustered at the firm level. Dependent variable is count of non-cybersecurity patents. Where a non-cybesecurity patent is a patent that is not classified as cybersecurity patent using our methodology. N refers to the total number of firm-year. *Cit-wtd CS patent* and *Val-wtd CS patent* are one-year lagged counts of cybersecurity patents. Cyber-risk score, and control variables are lagged by one year. Cyberrisk score measure is obtained from Florackis et al. (2023) and extended up to 2022. Value-weighted patent count is the sum of stock market value generated over all the patents filed by a firm in a year, scaled by total assets. For the description of control variables, see notes for Table 2.

Table 11: Regression with in-house cybersecurity firms

	Overall patent count		Non-CS patent count	
	Cit-wtd count (1)	Val-wtd count (2)	Cit-wtd count (3)	Val-wtd count (4)
Cyber risk score * (in-house CS = 0)	0.185	0.0390	0.147	0.0673
	(0.166)	(0.125)	(0.157)	(0.123)
Cyber risk score * (in-house CS = 1)	0.303**	0.287*	0.304**	0.294*
	(0.139)	(0.154)	(0.138)	(0.154)
Cit-wtd CS count	Yes	No	Yes	No
Val-wtd CS count	No	Yes	No	Yes
Size + other controls	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
N	13757	13757	13704	13704

$^{*}p < 0.10,^{**}p < 0.05,^{***}p < 0.01$.The coefficient estimates are derived from the Poisson pseudo-maximum likelihood estimation. Standard errors are denoted in parentheses and are clustered at the firm level. Here, N represents the total number of firm-year observations. A non-cybersecurity patent is defined as a patent that does not fall under the classification of cybersecurity patent according to our established methodology. The terms *Cit-wtd CS patent* and *Val-wtd CS patent* refer to one-year lagged counts of cybersecurity patents. Both the cyber risk score and control variables are lagged by one year. The measure for the cyberrisk score is derived from Florackis et al. (2023) and is extended up to 2022. Firms characterized as in-house cybersecurity firms are those that foster cybersecurity innovation internally. They are identified based on the citation of their own cybersecurity patents in their other patents. Value-weighted patent count encapsulates the aggregate stock market value generated by all the patents a firm files within a year, adjusted by total assets. For a detailed description of control variables, refer to the notes accompanying Table 2.

To evaluate our hypothesis, we regress the innovation outcomes against cyber risk, interacting with a dummy variable identifying in-house firms. Table 11 lays out the results, employing our two measures of innovation as dependent variables: citation-weighted patent count and value-weighted patent count. Column 1 reveals that the innovation of in-house firms reacts almost 1.7 times more robustly to cyber risk compared to out-house firms. When observing value-weighted patent counts (Column 2), the response disparity is even more pronounced — a staggering 13 times of the out-house firms.

Columns 3 and 4 of Table 11 delve deeper into how anti-cyber risk innovation diffuses to general innovation among in-house and out-house firms. Confirming our model prediction, our findings suggest that the growth in non-cyber security innovation in response to cyber risk is predominantly driven by in-house firms. Column 3 demonstrates that the response of in-house firms' non-cyber security innovation to cyber risk is twice as robust as that of out-house firms, in both citation-weighted and value-weighted counts. This trend remains consistent even when we apply a narrower definition to categorize in-house firms (results not presented).

3.10 Cyber risk and product innovation

In our model, innovation fundamentally manifests as an expansion in product varieties or enhancement in product quality. Hence, the explored innovation outcomes should also reflect in product innovation. To verify this, we pinpoint product patents filed by the firms in our sample. Product patents symbolize both the genesis of new products and enhancements in the quality of existing ones (Babina et al., 2023). Utilizing the patent claims dataset shared by Ganglmair et al. (2022), which classifies patent claims into product and process claims, we label a patent as a product patent if 50 percent or more of its claims are designated as product claims (Babina et al., 2023), and similarly define process patents.

We examine whether an escalation in cyber risk triggers an uptick in product patenting. Our testing methodology is twofold: initially, we regress product patent counts, and subsequently, we regress the ratio of product patent counts to process patent counts. Table 12 unveils the results of these regressions. Columns 1 and 2 affirm that a one s.d. hike in cyber risk catalyzes around a 7 percent increase in product innovation in terms of citation-weighted patent counts, and approximately a 9.7 percent increase in value-weighted terms. Further, we scrutinize whether the surge in product innovation

supersedes process innovation by analyzing the proportion of product patent counts in the aggregate (product patent count + process patent count). Columns 3 and 4 reveal that the fraction of product patents indeed ascends as firms confront elevated cyber risk.

Table 12: Regression of product patent count and share

	Product patent count		Share of product patents	
	Cit-wtd count	Val-wtd count	in cit-wtd count	in val-wtd count
	(1)	(2)	(3)	(4)
Cyberrisk score	0.244**	0.293***	0.0981**	0.0899**
	(0.106)	(0.113)	(0.0419)	(0.0406)
Cit-wtd CS count	Yes	No	Yes	No
Val-wtd CS count	No	Yes	No	Yes
Size + other controls	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
N	11804	11804	8504	8504

$^{*}p < 0.10,^{**}p < 0.05,^{***}p < 0.01$. The coefficient estimates are derived from the Poisson pseudo-maximum likelihood estimation. Standard errors are denoted in parentheses and are clustered at the firm level. Here, N represents the total number of firm-year observations. Product patents are defined as those having at least 50% of their claims categorized as product claims according to Ganglmair et al. (2022). The term 'Share' represents the proportion of product patents in the total patent count, which includes both product and process patents. The terms *Cit-wtd CS patent* and *Val-wtd CS patent* refer to one-year lagged counts of cybersecurity patents. Both the cyber risk score and control variables are lagged by one year. The measure for the cyberrisk score is derived from Florackis et al. (2023) and is extended up to 2022. Value-weighted patent count encapsulates the aggregate stock market value generated by all the patents a firm files within a year, adjusted by total assets. For a detailed description of control variables, refer to the notes accompanying Table 2.

To delve into the mechanism at play, and in alignment with our model, we lay our focus on the firms with in-house cyber security innovation. Additionally, we aim to discern if, among the in-house firms, it's the data-intensive entities that exhibit the most pronounced product market innovation. To achieve this, we perform a triple interaction involving the in-house dummy, a dummy for data-intensiveness, and the cyber risk score. Table 13 illustrates that the most substantial response to cyber risk emanates from data-intensive firms possessing in-house cyber security, followed by non-data-intensive firms with in-house cyber security innovation, and then by data-intensive firms lacking in-house cyber security. Conversely, non-data-intensive firms devoid of in-house cyber security innovation trail in product innovation in reaction to cyber risk.

Table 13: Regression of product patent count and share with in-house and data-intensive firms

	Product patent count		Share of product patents	
	Cit-wtd count	Val-wtd count	in cit-wtd count	in val-wtd count
	(1)	(2)	(3)	(4)
Cyberrisk score * (in-house = 0 & dataint = 0)	-0.0185	0.0957	0.0604	0.0467
	(0.169)	(0.151)	(0.0456)	(0.0444)
Cyberrisk score * (in-house = 0 & dataint = 1)	-0.154	0.0420	0.0466	0.0388
	(0.338)	(0.225)	(0.0964)	(0.0942)
Cyberrisk score * (in-house = 1 & dataint = 0)	0.300*	0.624***	0.139**	0.141**
	(0.170)	(0.228)	(0.0571)	(0.0582)
Cyberrisk score * (in-house = 1 & dataint = 1)	0.480***	0.628***	0.257***	0.256***
	(0.157)	(0.189)	(0.0862)	(0.0783)
Cit-wtd CS count	Yes	No	Yes	No
Val-wtd CS count	No	Yes	No	Yes
Size + other controls	Yes	Yes	Yes	Yes
Firm FE	Yes	Yes	Yes	Yes
Year FE	Yes	Yes	Yes	Yes
N	11804	11804	8504	8504

$^{*}p < 0.10$,$^{**}p < 0.05$,$^{***}p < 0.01$. The coefficient estimates are derived from the Poisson pseudo-maximum likelihood estimation. Standard errors are denoted in parentheses and are clustered at the firm level. Here, N represents the total number of firm-year observations. Product patents are defined as those having at least 50% of their claims categorized as product claims according to Ganglmair et al. (2022). The term 'Share' represents the proportion of product patents in the total patent count, which includes both product and process patents. The terms *Cit-wtd CS patent* and *Val-wtd CS patent* refer to one-year lagged counts of cybersecurity patents. Both the cyber risk score and control variables are lagged by one year. The measure for the cyberrisk score is derived from Florackis et al. (2023) and is extended up to 2022. Firms characterized as in-house cybersecurity firms are those that foster cybersecurity innovation internally. They are identified based on the citation of their own cybersecurity patents in their other patents. Data-intensive firms are identified as those actively engaged in AI innovation or those mirroring AI innovating firms in terms of their business description. Value-weighted patent count encapsulates the aggregate stock market value generated by all the patents a firm files within a year, adjusted by total assets. For a detailed description of control variables, refer to the notes accompanying Table 2.

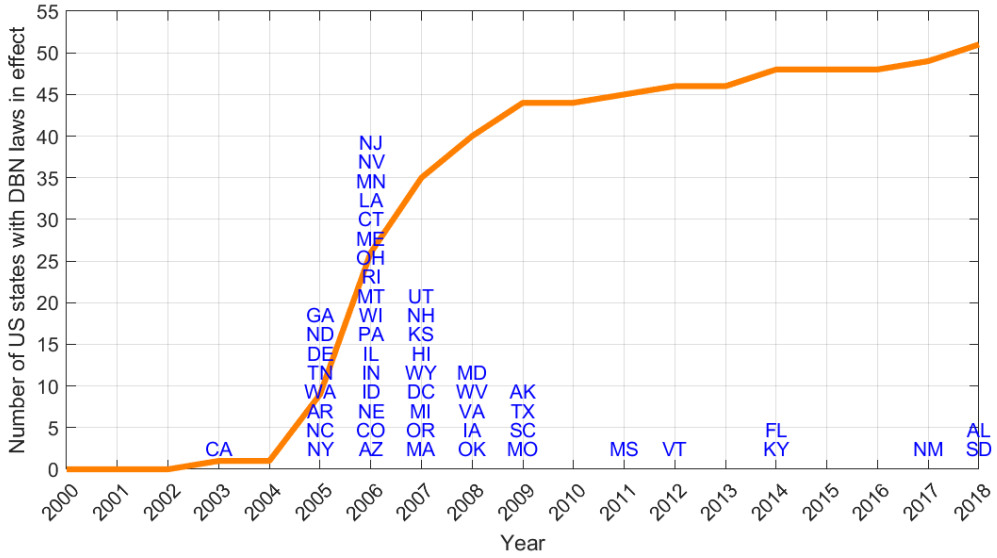
4 Addressing Endogeneity

In the previous section we investigated the direct impact of an increase in cyber risk on firm innovation activities. However, there exists an endogeneity problem in assessing the impact of cyber risk on firm innovation due to intertwined relationships where cyber risk and innovation mutually influence each other, making it challenging to establish a clear cause-and-effect relationship. For instance, while cyber risks might hinder innovation by diverting resources toward cyber security measures, innovative activities within a firm could also lead to increased cyber risks due to new technologies or processes being introduced. Moreover, firms that are more innovative might invest more in advanced technologies, making them both more susceptible to cyber risks and more likely to innovate. This bias can create a spurious relationship between cyber risk and innovation if not properly addressed. Factors such as reverse causality, omitted variables, simultaneity, and sample selection bias complicate the distinction between the effects of cyber risk on innovation and vice versa.

In this section, to address this issue, we employ an instrumental variables approach to disentangle and understand the true causal impact of cyber risk on firm innovation

activities. Our instrument is going to be the adoption of Data Breach Notification Laws in the United States, which have been shown to increase firm risk related to data breaches (Boasiako and Keefe (2021); Liu and Ni (2023); Huang and Wang (2021)).

Figure 2: State adoption of DBN laws



Legend: This figure reports the first time in each state and district that a data breach notification law is enacted specifically containing data security breach notification provisions. For example, Nevada introduced a data breach statute in January 2005, but it only required notification provisions for general data provisions in January 2006; thus, in our sample, it appears as a 2006 adoption of DBN law. Only in Nevada also is the ability to launch a private action (2005) different from the date of DBN law adoption. Other states that allow for a private cause of action are: Alabama, Alaska, California, Delaware, D.C., Hawaii, Idaho, Illinois, Louisiana, Maryland, Massachusetts, Minnesota, Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Washington, and Wisconsin. The source of the data is Perkins Coie (see https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html).

Data Breach Notification Laws (DBNL) in the United States mandate firms to inform individuals affected by a data breach involving their personal information. Typically, these laws require companies that experience a data breach to notify affected individuals within a specified time-frame, often ranging from 30 to 90 days after the breach is discovered. The notification usually includes details about the nature of the breach, the type of information compromised, and steps individuals can take to protect themselves. Additionally, some states require organizations to notify state authorities or consumer reporting agencies depending on the scale and severity of the breach. The laws also have provisions outlining penalties for non-compliance, aiming to hold organizations accountable for safeguarding individuals' personal data. All 50 states have

enacted their own versions of DBNL starting in 2003 with California and ending in 2018 with Alabama and South Dakota. By 2008, more than half of the states had adopted a DBN law, as shown in Figure (2).

Our empirical strategy is going to explore the staggered implementation of Data Breach Notification Laws (DBNL) in the United States, which increased firm risk, and compare the innovation activities of firms located in early-treated states to those of firms located in late-treated states. A very recent literature (Baker et al. (2022); Goodman-Bacon (2021), among others) has uncovered two vital econometric issues in standard staggered difference-in-difference methods such as linear two-way fixed effects (henceforth, TWFE): (1) there is a possibility of bias due to "forbidden comparisons", and (2) there is a possibility of bias and/or inefficiency due to misspecification in the presence of right skewed dependent variables. For example, related to the first issue, standard dynamic two-way fixed effects methods suffer from a problem that it aggregates treatment effects over some valid comparisons but also over some "forbidden" comparisons. Specifically, it also compares already treated units (as controls) with the later treated units (as treated). When the treatment effects are heterogeneous over time or across treatment units, it may lead to biased average treatment effect in the treated (ATT) estimates. The second issue of misspecification in the presence of right skewed dependent variable is also a serious issue. Using a $log(1 + y)$ transformation of the dependent variable, a log-linear, or an inverse hyperbolic sine (IHS) regression produces inconsistent and biased estimates. Another method to reduce skewness, the negative binomial regression, does not work with fixed effects.

This leaves us with three models that admit fixed effects and produce unbiased estimates: linear, Poisson, and rate regression. The literature has shown that the Poisson regression is the best because it is the most efficient, having the lowest variance among these three unbiased strategies. In the Appendix, we show the results of a Poisson two-way fixed effects analysis for completeness. Linear regressions can be admitted, however, in spite of problems of high variance, because there are no issues of bias and inconsistency (Cohn et al. (2022)). This will make it harder to get significant results, but at least the estimates will be unbiased and consistent with correct sign. Positive significant results will suggest that *despite* the method producing high variance estimates, there is evidence of an effect of data breach notification laws on firm innovation activities.

In our analysis, we use the Borusyak et al. (2022) linear method (henceforth, BJS) that addresses the first challenge of "forbidden comparisons" and is unbiased

and consistent (Cohn et al. (2022)), despite being inefficient. Other popular methods that account for "forbidden comparisons" are Callaway and Sant'Anna (2021), Sun and Abraham (2021), and de Chaisemartin et al. (2020), among others. The BJS estimator is the most efficient under the assumption of parallel trends because it uses all of pre-treatment data in estimation and it is robust to cases when treatment effects vary arbitrarily. The first estimation that we run is a linear difference-in-differences regression accounting for "forbidden comparisons" using the BJS 3-step imputation representation for the efficient estimator, explained below:

1. Within the untreated observations only, estimate the λ_i and δ_t (by $\hat{\lambda}_i^\star$, $\hat{\delta}_t^{\,\star}$) by OLS in
$$Y_{it} = \lambda_i + \delta_t + \epsilon_{it}, \tag{2}$$
where λ_i is unit (i.e. firm) fixed effect, δ_t is year fixed effect;

2. For each treated observation with $w_{it} \neq 0$, set $\hat{Y}_{it} = \hat{\lambda}_i^\star + \hat{\delta}_t^{\,\star}$ and $\hat{\tau}_{it}^\star = Y_{it} - \hat{Y}_{it}(0)$ to obtain the estimate of τ_{it};

3. Estimate the target τ_w by a weighted sum $\hat{\tau}_w^\star = \sum_{it} w_{it}\hat{\tau}_{it}^\star$;

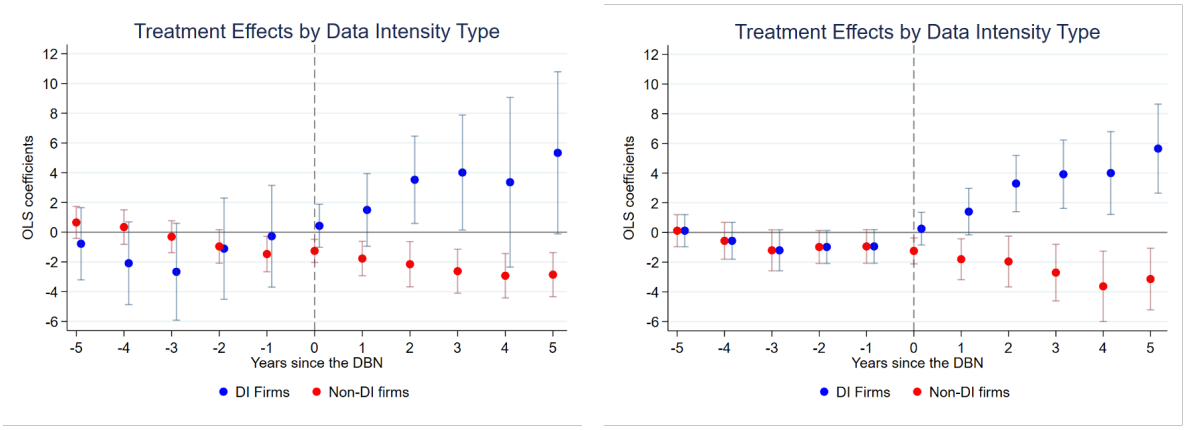
The above model allows us to estimate unbiased and consistent dynamic treatment effects using panel data on firms i over years t, where Y_{it} is the time t firm-level measure of innovation, $Y_{it}(0)$ is the period-t stochastic potential outcome of unit i if it is never treated, $\Omega_1 = \{it \in \Omega | treated = 1\}$ is the set of treated observations (i.e., firms are headquartered in a state that has adopted a DBN law), $\Omega_0 = \{it \in \Omega | treated = 0\}$ is the set of untreated (i.e., never-treated and not-yet-treated) observations, $\tau_{it} = \mathbb{E}[Y_{it} - Y_{it}(0)]$ represents the causal effects on the treated observations $it \in \Omega_1$, w_{it} are BJS-derived pre-specified non-stochastic weights that depend on treatment assignment and timing, but not on realized outcomes.

4.1 Data-intensive firms.

Figure (3) presents the BJS-weighted dynamic heterogeneous treatment effects of citation-weighted patent counts by firm data-intensity (DI). The left-hand panel allows heterogeneous pre-trends, while the right-hand panel assumes common pre-trends for both groups, but estimates ATT separately post-treatment.

As shown in Figure (3), data-intensive firms exhibit higher overall innovation after the adoption of DBN laws. On the other hand, non-data intensive firms exhibit lower overall innovation after the adoption of DBN laws, suggesting the adoption of these laws is a significant negative shock for firms that imposes high costs which overall discourage innovation. It is to be noted that both panels provide evidence on the observed counterparts of the parallel trends assumption and show that we do not have an unnatural experiment.

Figure 3: Citation-weighted patent count by data intensity (DI).



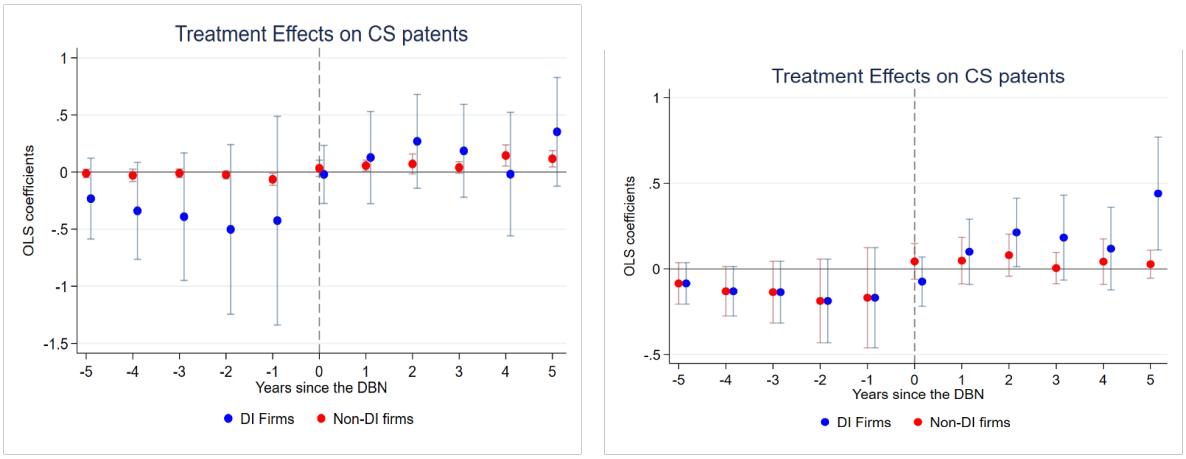
Legend: This figure plots BJS-weighted dynamic heterogeneous treatment effects of citation-weighted patent counts by firm data-intensity (DI) pre- and post- treatment. The '0' event is the staggered adoption of DBN laws across the United States. Data intensive firms are identified using a combination of the USPTO dataset on AI patents (Giczy et al. (2022)) and the KPSS patent dataset linked to firms (Kogan et al. (2017)). Moreover, firms that are close to AI patenting firms in the sense of Hoberg and Phillips (2016) and mirror their AI innovations are also considered data-intensive. This measure has the advantage to be constructed from entirely publicly available data and it is different from IT expenditures.

Figure (4) presents the BJS-weighted dynamic heterogeneous treatment effects of citation-weighted *cybersecurity* patent counts by firm data-intensity (DI). The left-hand panel allows heterogeneous pre-trends, while the right-hand panel assumes common pre-trends for both groups, but estimates ATT separately post-treatment.

As shown in Figure (4), data-intensive firms exhibit a slight increase in cybersecurity patenting, although the results are not significant except for long-term horizons. The insignificance of results is due to there being very few firms overall that produce cybersecurity patents.

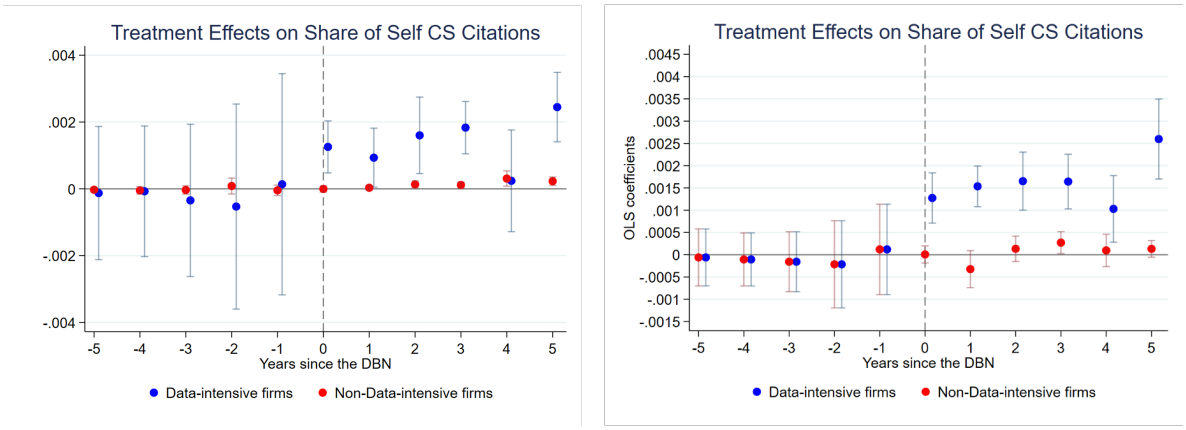
While data-intensive firms seem to modestly increase their overall issuance of cybersecurity patents, in particular at longer horizons, we also investigate whether their share of *self*-cybersecurity patent citations increases after the adoption of DBN laws.

Figure 4: Citation-weighted *cybersecurity* patent count by data intensity (DI).



Legend: This figure plots the effects of citation-weighted cybersecurity patent counts by firm data-intensity (DI) pre- and post- treatment. The '0' event is the staggered adoption of DBN laws across the United States. Estimates for data intensive (DI) firms are in blue, while estimates for non-data intensive (non-DI) firms are in red. Data intensive firms are identified as described previously.

Figure 5: Share of *self*-cybersecurity patent citations by data intensity (DI).



Legend: This figure plots the effects of the share of *self*-cybersecurity patent citations by firm data-intensity (DI) pre- and post- treatment. The '0' event is the staggered adoption of DBN laws across the United States. Estimates for data intensive (DI) firms are in blue, while estimates for non-data intensive (non-DI) firms are in red. Data intensive firms are identified as described previously.

As shown in Figure (5), the share of *self*-cybersecurity patent citations for data-intensive firms increases on impact, while the share of *self*-cybersecurity patent citations for non-data-intensve firms stays flat. This suggests that data-intensive firms cite their own cybersecurity patents much more often after the adoption of DBN laws.

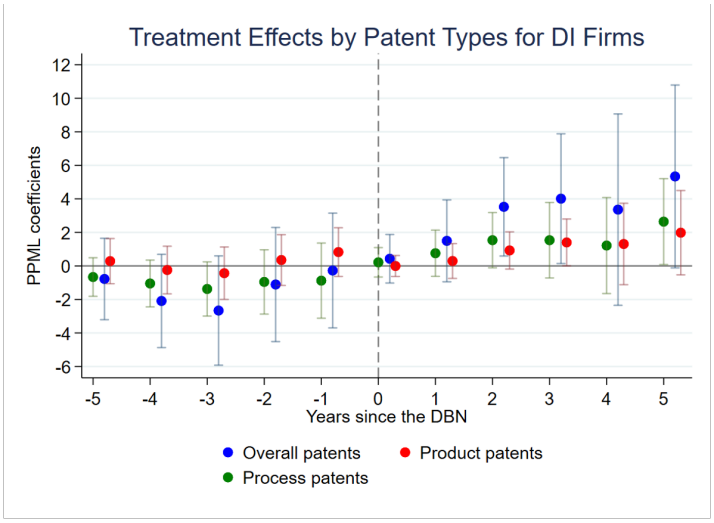
Lastly, we also examine differences in patent type (product vs. process patents) after the adoption of DBN laws. In our model, innovation primarily appears as an expansion of product varieties or improvements in product quality. Therefore, the outcomes of innovation that we are investigating should be evident in terms of product innovation.

To validate this, we refocus on the product patents filed by the companies in our study. Product patents signify both the introduction of new products and enhancements in the quality of existing ones (Babina et al. (2023)). To identify these patents, we utilize the patent claims dataset provided by Ganglmair et al. (2022), which categorizes patent claims into product and process claims. We classify a patent as a product patent if 50 percent or more of its claims are specified as product claims, following the method described in Babina et al. (2023). Similarly, we establish the definition of process patents in a similar manner.

Figure (6) presents the BJS-weighted dynamic heterogeneous treatment effects of citation-weighted patent counts by patent type (i.e., overall, product, and process) for data-intensive firms. The left-hand panel allows heterogeneous pre-trends, while the right-hand panel assumes common pre-trends for both groups, but estimates ATT separately post-treatment.

As shown in Figure (6), data-intensive firms exhibit a slight increase in cyber-security patenting, although the results are not significant except for long-term horizons. As mentioned previously, linear staggered diff-in-diff methods that account for 'forbidden comparisons' produce consistent and unbiased estimates, but they may produce insignificant estimates due to high variances, when the dependent variable is right skewed, which is typical of the patent counts.

Figure 6: Citation-weighted patent count: by patent type, for data-intensive firms



Legend: This figure plots the effects of citation-weighted cybersecurity patent counts by firm data-intensity (DI) pre- and post- treatment. The '0' event is the staggered adoption of DBN laws across the United States. Estimates for data intensive (DI) firms are in blue, while estimates for non-data intensive (non-DI) firms are in red. Data intensive firms are identified as described previously.

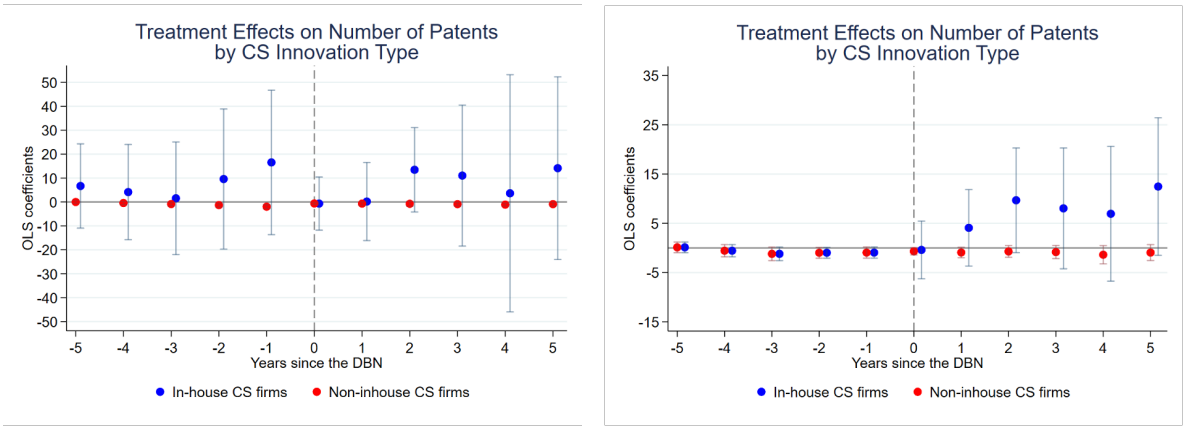
4.2 In-house cybersecurity firms.

Figure (7) repeats the exercise of examining firms' overall patenting behavior by the firm's choice of in-house versus external cybersecurity protection. As shown in Figure (7), in-house cybersecurity firms exhibit a slight increase in cyber-security patenting, although the results are not significant except for long-term horizons again.

Figure (8) presents the BJS-weighted dynamic heterogeneous treatment effects of citation-weighted overall patent counts by firm data-intensity (DI) interacted with in-house cybersecurity (in-house CS) protection choices. The left-hand panel allows heterogeneous pre-trends, while the right-hand panel assumes common pre-trends for both groups, but estimates ATT separately post-treatment.

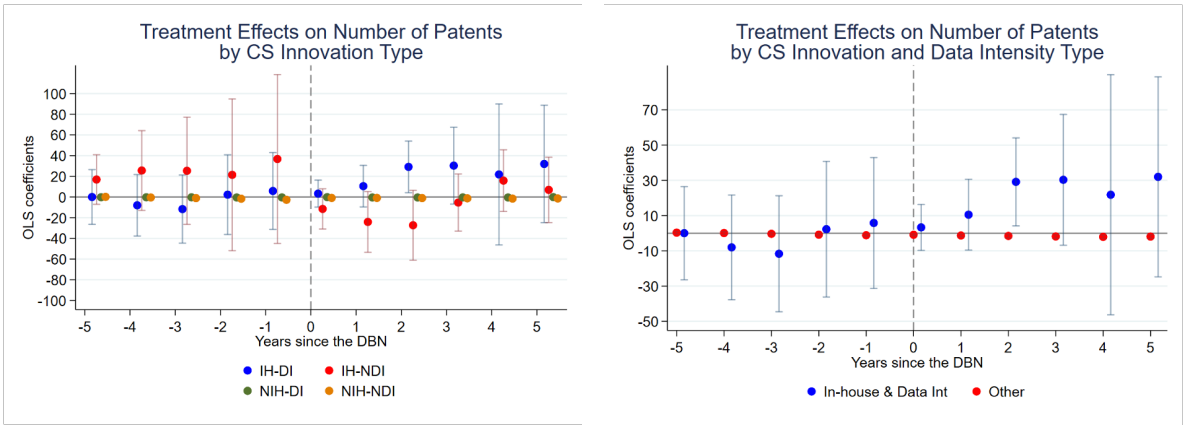
As shown in Figure (8), firms that use both in-house cyberprotection and are data-intensive exhibit a slight increase in cyber-security patenting, although the results are not significant.

Figure 7: Citation-weighted patent count by in-house vs. external cyberprotection.



Legend: This figure plots BJS-weighted dynamic heterogeneous treatment effects of citation-weighted cybersecurity patent counts by firm's choice of in-house vs. external cybersecurity protection pre- and post- treatment. The '0' event is the staggered adoption of DBN laws across the United States. Estimates for in-house cybersecurity (in-house CS) firms are in blue, while estimates for non-in-house cybersecurity (non-in-house CS) firms are in red. In-house cybersecurity firms are identified if they cite at least one of their own cybersecurity patents in their general patents.

Figure 8: Citation-weighted patent count, data intensity interacted with in-house protection

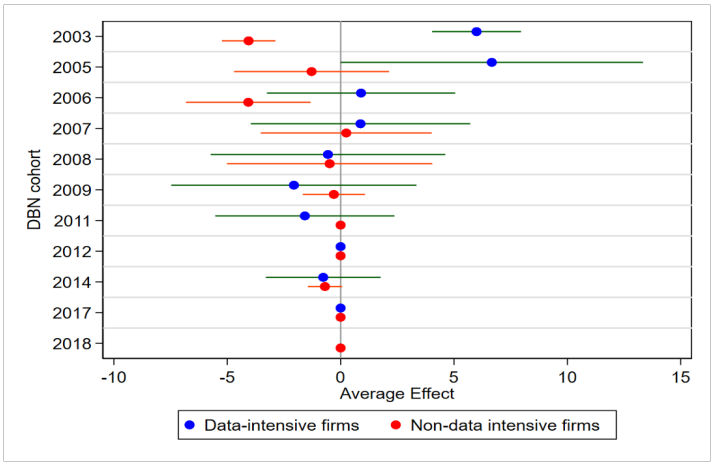


Legend: This figure plots BJS-weighted dynamic heterogeneous treatment effects of citation-weighted cybersecurity patent counts by firm's choice of in-house vs. external cybersecurity protection interacted with data-intensity pre- and post- treatment. The '0' event is the staggered adoption of DBN laws across the United States. Estimates for in-house cybersecurity (in-house CS) firms are in blue, while estimates for non-in-house cybersecurity (non-in-house CS) firms are in red. In-house cybersecurity firms are identified if they cite at least one of their own cybersecurity patents in their general patents. Data intensity firms are identified as mentioned previously.

4.3 Cohort effects

We also examine whether firms' innovation changes after the adoption of DBN laws depending on the cohort. This could happen if later treated cohorts anticipate DBN law adoption in their state. In that case, the estimates will be smaller for later treated cohorts. It could also happen if the nature of cyberrisk has changed over time in such a way that first movers had an advantage. Moreover, if cyberrisk has changed in nature and severity over the last twenty years, it could be that it became too costly for later treated cohorts to invest resources into growth and innovation because too many resources had to go directly in managing cyberrisk and actual cyberattacks. While we cannot distinguish between these mechanisms empirically, they all could be at play at the same time.

Figure 9: Treatment effects by cohort (= year of DBN Implementation)

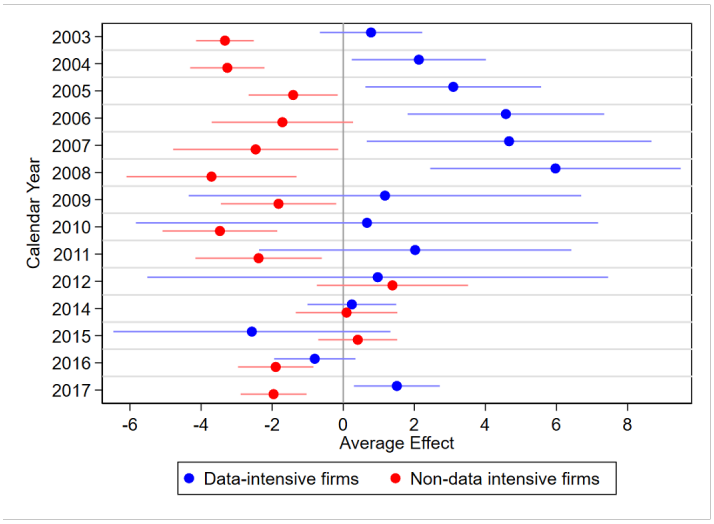


Legend: This figure plots treatment effects by cohort for data-intensive and non-data intensive firms. Estimates for data intensive firms (DI) are in blue, while estimates for non-data intensive (non-DI) firms are in red. Data intensity firms are identified as mentioned previously.

Figure (9) shows that, indeed, the very earliest treated data-intensive cohorts responded the most. These effects are averaged all the post-treatment years.

In Figure (10) we explore the DBN law effects in a particular year. The period 2004 to 2008 is the most intense period in terms of increase in firms' innovation activities in response to the increase in cyberrisk, as measured by DBN laws.

Figure 10: Treatment effects by calendar year



Legend: This figure plots treatment effects by calendar year for data-intensive and non-data intensive firms. Each estimate is the sum of effects of all treated cohorts up to and including that year in that particular year. So for instance 2008 will contain the effect for 3rd year since the firms treated in 2005, 2nd year effects for firms treated in 2006 and so on. Estimates for data intensive firms (DI) are in blue, while estimates for non-data intensive (non-DI) firms are in red. Data intensity firms are identified as mentioned previously.

5 A model of big data, cybercrime and cyber security

5.1 Efficient data use and security risks

We consider a competitive industry. Time is discrete and infinite. There is a continuum of firms indexed by i. Each firm i produces a good of quality $A_{i,t}$.

$$y_{i,t} = A_{i,t}. \tag{3}$$

Because the single input employed in production is one unit of capital, variable $A_{i,t}$ also represents the real value of the producer's output.

Quality $A_{i,t}$ depends on a firm's choice of a production technique $a_{i,t}$, which can be interpreted as managing inventories, or learning about consumers' tastes. In each period, and for each firm, there is one optimal technique with a persistent and a transitory components: $\theta_{i,t} + \epsilon_{a,i,t}$. The persistent component $\theta_{i,t}$ is unknown and follows an AR(1) process, where $\eta_{i,t}$ is *i.i.d.* across time and firms:

$$\theta_{i,t} = \bar{\theta} + \rho(\theta_{i,t-1} - \bar{\theta}) + \eta_{i,t}. \tag{4}$$

Firms have a noisy prior about the realization of θ_0. The transitory shock $\epsilon_{a,i,t}$ is *i.i.d.* across time and firms and is unlearnable. Deviating from that optimum incurs a quadratic loss in quality:

$$A_{i,t} = \bar{A}_i - (a_{i,t} - \theta_{i,t} - \epsilon_{a,i,t})^2. \tag{5}$$

Quality $A_{i,t}$ is a strictly decreasing function of the difference between the firm's chosen production technique, $a_{i,t}$, and the optimal technique $\theta_{i,t} + \epsilon_{a,i,t}$. A decreasing function means that techniques far away from the optimum result in worse quality goods.

Data as by-product. Data helps firms infer $\theta_{i,t}$ Term ϵ_a indicates that firms are incapable of fully inferring $\theta_{i,t}$ at the end of each period; it makes the accumulation of past data a valuable asset. If a firm knew the current value of $\theta_{i,t}$, it would maximize quality by setting $a_{i,t} = \theta_{i,t}$.

In our model, similar to Farboodi et al. (2019) and Farboodi and Veldkamp (2021), data is a by-product of economic activity. Each firm passively obtains z data points as

a by-product of production. Each data point $m \in [1:z]$ reveals

$$s_{i,t,m} = \theta_{i,t} + \epsilon_{i,t,m}, \tag{6}$$

where $\epsilon_{i,t,m}$ is *i.i.d.* across firms, time, and signals. For tractability, we assume that all the shocks are normally distributed: fundamental uncertainty is $\eta_{i,t} \sim N(\mu, \sigma_\theta^2)$, signal noise is $\epsilon_{i,t,m} \sim N(0, \sigma_\epsilon^2)$, and the unlearnable quality shock is $\epsilon_{a,i,t} \sim N(0, \sigma_a^2)$.

Cyber risk. Data is subject to cybercrime or cyber incident risk, meaning that it can be lost and, in that case, it can no longer be used for prediction. We denote the risk of cybercrime by $\vartheta \in [0, 1]$. With probability ϑ, a firm risks losing all its data, while with probability $(1 - \vartheta)$ the firm keeps its data generated as a by-product of activity, $z\sigma_\theta^2$. Thus, the data endowment under cyber risk is $(1 - \vartheta)z\sigma_\epsilon^2$.

Cybersecurity. A key assumption of our model is that firms are heterogeneous in their capability to protect themselves against cybercrime. High capability (H-type) firms can develop in-house cyber security protection, while low capability (L-type) firms cannot develop this security internally, but can buy it externally from H-type firms.

The essential distinction between in-house and external cyber security is that internal cyber security can also be used to innovate, besides providing protection against cyber-attacks. This is because in-house cyber security is typically more easily integrated with existing R&D and product development systems, and tends to be more tailored for a firms' specific business needs. In the model, innovation is modeled as an increase in the productivity ceiling $\overline{A}_i$.

Low-type capability firms do not generate in-house security, but they can buy it externally from Hig$H$-type firms. In this case, they can only use it to mitigate the impact of cyberrisk and not to innovate (i.e., they can use the security software for protecting their production process, but their R&D department does not know and is unable to use the security software for product improvements).

Let m_H represent the share of H-type firms. Aggregate output is then the sum of weighted outputs for the two types of firms:

$$Y_t = \int_0^1 A_{i,t} di = m_H A_{H,t} + (1 - m_H) A_{L,t}. \tag{7}$$

Let $\tau_t \geq 0$ represent the investment in in-house cyber security made by a firm of

the H-type. Let also $\delta_t \geq 0$ represent the amount of external cyber security bought by a firm of the L-type from the H-type firms at an endogenous price denoted by π. Given the firms' shares, the amount of protection that is sold by a H-type producer must be $\frac{1-m_H}{m_H}\delta_t$. In this case, on the aggregate H-firms sell $(1-m_H)\delta_t$, which is precisely the value of protection purchased by the universe of L-type firms.

Nonrivlary. When a company invests in cyber security measures such as firewalls, encryption protocols, or security software, these measures protect the company's data and systems without necessarily reducing their effectiveness for other companies that may use similar security tools. This suggests that cyber security is (partially) nonrival.

Thus, we assume that when an H-type firm sells a given amount of cyber protection, it retains, for its own use, a share $1-\iota$ of such protection, where $\iota \in (0,1)$. Therefore, the H-firm that invests τ_t in cyber security and trades $\frac{1-m_H}{m_H}\delta_t \leq \tau_t$, will retain, for its own use, $\tau_t - \iota\frac{1-m_H}{m_H}\delta_t$. This amount of cyber protection can be used to mitigate the impact of cyber risk, transforming the term $(1-\vartheta)z$ into $\left[1-\vartheta e^{-\left(\tau_t-\iota\frac{1-m_H}{m_H}\delta_t\right)}\right]z$. Note that if $\tau_t - \iota\frac{1-m_H}{m_H}\delta_t = 0$, there is no use of cyber protection, and the effect of cyber risk over data is maximum; if $\tau_t - \iota\frac{1-m_H}{m_H}\delta_t \to \infty$, then there is full protection, and the original data endowment maintains its integrity.

Firm problem. With this in mind, we can write firm i's optimization problem, where $i \in \{H, L\}$. As mentioned previously, the H-type firm can use the investment in cyber security to enhance the potential quality of the produced good. Hence, constant $\overline{A}_i$ is replaced, for this type of firm, by the term $\overline{A}e^{b\left(\tau_t-\iota\frac{1-m_H}{m_H}\delta_t\right)}$.

An H-type firm chooses a sequence of quality decisions $a_{i,t}$, in-house cyber security investments τ_t, and how much cyber security δ_t to sell at price π_t to maximize:

$$\mathbb{E}_0 \sum_{t=0}^{\infty} \beta^t \left[\overline{A}e^{b\left(\tau_t-\iota\frac{1-m_H}{m_H}\delta_t\right)} - (a_{i,t}-\theta_{i,t}-\epsilon_{a,i,t})^2 - \tau_t + \frac{1-m_H}{m_H}\delta_t\pi_t - r\right] \tag{8}$$

An L-type firm chooses a sequence of quality decisions $a_{i,t}$, and how much external cybersecurity protection δ_t to buy at price π_t to maximize:

$$\mathbb{E}_0 \sum_{t=0}^{\infty} \beta^t \left[\bar{A} - (a_{i,t}-\theta_{i,t}-\epsilon_{a,i,t})^2 - \delta_t\pi_t - r\right] \tag{9}$$

Note the differences between the two expressions: innovation from cyber security is possible for the H-type firm but not for the L-type firm ; the cost of investment in cyber security is present only in the H-type firm expression; protection trading is a revenue for those who sell it and a cost for those who buy it.

The stock of knowledge. The information set of firm $i \in \{H, L\}$ when it chooses its technique $a_{i,t}$ is $\mathcal{I}_{i,t} = \{\mathcal{I}_{i,t-1}, \{s_{i,t-1,m}\}_{m=1}^{z}, A_{i,t-1}\}$ where z is the net numbers of points added each period as a by-product of economic activity. To make the problem recursive, we construct a helpful summary statistic for this information, called the "stock of knowledge." A firm's stock of knowledge is the inverse of its posterior variance, or in other words, the precision of firm i's forecast of θ_t, which is formally:

$$\Omega_{i,t} = \mathbb{E}\left[(\mathbb{E}[\theta_t|\mathcal{I}_{i,t}] - \theta_t)^2\right]^{-1} \tag{10}$$

Note that the inside of the expression is the difference between a forecast, $\mathbb{E}[\theta_t|\mathcal{I}_{i,t}]$ and the realized value, θ_t, and is therefore a forecast error. An expected squared forecast error is the variance of the forecast. It is also called the variance of θ_t, conditional on the information set $\mathcal{I}_{i,t}$, or the posterior variance. The inverse of a variance is a precision. Thus, this is the precision of firm i's forecast of θ_t.

5.2 A law of motion for knowledge

The state variables of the recursive problems in (8) and (9) are the prior mean and variance of beliefs about $\theta_{i,t-1}$, and the new data points. Taking a first order condition with respect to the technique choice, we find that the optimal technique is $a^*_{i,t} = \mathbb{E}_i[\theta_{i,t}|\mathcal{I}_{i,t}]$. Given the posterior variance of beliefs in equation (10), the expected quality for the H-type and the L-type firms, respectively, are

$$\mathbb{E}[A_{H,t}] = \overline{A}e^{b\left(\tau_t - \iota\frac{1-m_H}{m_H}\delta_t\right)} - \Omega_{H,t}^{-1} - \sigma_a^2 \tag{11}$$

$$\mathbb{E}[A_{L,t}] = \overline{A} - \Omega_{L,t}^{-1} - \sigma_a^2 \tag{12}$$

Deriving the law of motion for the stock of knowledge, $\Omega_{i,t}$, requires adding new data from two sources: 1) data as a by-product of production, which is subject to cyberrisk but can be protected through cyber security and 2) data inferred from a firm observing its own quality at the end of a production period. These two pieces of information are

incorporated into beliefs using Bayes' law.

Each firm $i \in \{H, L\}$ observes $z_i = z$ data points as a by-product of economic activity. This means that the sum of the precisions of all the signals (data proints), $z_i \sigma_\epsilon^{-2}$ is part of the stock of knowledge. Both types of firms, the H-type and the L-type, are subject to cyberrisk, which can be reduced through protection. The H-type firm reduces cyberrisk by the amount of cybersecurity it retains for its own use, $\tau_t - \iota \frac{1-m_H}{m_H} \delta_t \leq \tau_t$, after it invests τ_t in cybersecurity and trades $\frac{1-m_H}{m_H} \delta_t \leq \tau_t$ cyber protection which is non-rival. This amount of cyberprotection can be used to mitigate the impact of cyberrisk, implying that the weighted sum of precisions of data points obtained as a byproduct of economic activity, subject to cyberrisk and after optimal cybersecurity decisions, is $\left[1 - \vartheta e^{-\left(\tau_t - \iota \frac{1-m_H}{m_H} \delta_t\right)}\right] z \sigma_\epsilon^{-2}$. L-type firm buys protection in amount δ_t and, therefore, the weighted sum of precisions of data points obtained as a byproduct of economic activity, subject to cyberrisk and after optimal cybersecurity decisions, is $\left[1 - \vartheta e^{-\delta_t}\right] z \sigma_\epsilon^{-2}$.

Moreover, each firm $i \in \{H, L\}$ is also learning from seeing its own realization of quality $A_{i,t}$ at the end of each period t, with precision σ_a^{-2}. This information is different from the produced data because the quality realization is a signal about θ_t, not about θ_{t+1}. Therefore, σ_a^{-2} gets added to the time-t stock of knowledge and depreciates, just like other time-t knowledge that the firm takes with it to time $t+1$.

Lemma (1) expresses the dynamic knowledge constraint that puts together data depreciation and data inflows.

Lemma 1 *The dynamic knowledge constraint is, for the H-type firm:*

$$\Omega_{H,t+1} = \left[\rho^2 (\Omega_{H,t} + \sigma_a^{-2})^{-1} + \sigma_\theta^2\right]^{-1} + \left[1 - \vartheta e^{-\left(\tau_t - \iota \frac{1-m_H}{m_H} \delta_t\right)}\right] z \sigma_\epsilon^{-2} \tag{13}$$

The L-type firm buys protection in amount δ_t and, therefore,

$$\Omega_{L,t+1} = \left[\rho^2 (\Omega_{L,t} + \sigma_a^{-2})^{-1} + \sigma_\theta^2\right]^{-1} + \left(1 - \vartheta e^{-\delta_t}\right) z \sigma_\epsilon^{-2} \tag{14}$$

In this last case, if the firm buys no protection, data loss risk occurs in a share ϑ; if it buys infinite protection, it faces no cyberrisk.

The demonstration for this lemma and all subsequent lemmas and propositions can be found in the Appendix. The proof involves utilizing Bayes' law, or alternatively, the Ricatti equation within a modified Kalman filter framework. Given the similarity in

information structure to that of a Kalman filter, the sequence of conditional variances (or conversely, their inverses, the sequence of precisions) is deterministic.

5.3 Recursive representation of the firm's problem, equilibrium and steady state

Lemma (2) proceeds with the recursive representation of the expected firm value.

Lemma 2 *The optimal sequences of in-house cyber security investments* $\{\tau_t\}$ *and cyber security sales* $\{\delta_t\}$ *solve the following current-value Hamiltonian function for the* H*-type firm:*

$$H_{H,t}(\Omega_{H,t},\tau_t,\delta_t,p_{H,t}) = \overline{A}e^{b\left(\tau_t-\iota\frac{1-m_H}{m_H}\delta_t\right)} - \Omega_{H,t}^{-1} - \sigma_a^2 - \tau_t + \frac{1-m_H}{m_H}\delta_t\pi_t - r + \tag{15}$$
$$+ \beta p_{H,t+1}(\Omega_{H,t+1}-\Omega_{H,t})$$
$$\text{where}\quad \Omega_{H,t+1} = \left[\rho^2(\Omega_{H,t}+\sigma_a^{-2})^{-1}+\sigma_\theta^2\right]^{-1} + \left[1-\vartheta e^{-\left(\tau_t-\iota\frac{1-m_H}{m_H}\delta_t\right)}\right] z\sigma_\epsilon^{-2} \tag{16}$$

and $p_{H,t}$ *is the shadow-price or co-state variable associated with the state variable, and the transversality condition is* $\lim_{t\to\infty}\Omega_{H,t}\beta^t p_{H,t}=0$.

The optimal sequence of cybersecurity purchases $\{\delta_t\}$ *solve the following current-value Hamiltonian function for the* L*-type firm:*

$$H_{L,t}(\Omega_{L,t},\tau_t,\delta_t,p_{L,t}) = \overline{A} - \Omega_{L,t}^{-1} - \sigma_a^2 - \delta_t\pi_t - r + \beta p_{L,t+1}(\Omega_{L,t+1}-\Omega_{L,t}) \tag{17}$$
$$\text{where}\quad \Omega_{L,t+1} = \left[\rho^2(\Omega_{L,t}+\sigma_a^{-2})^{-1}+\sigma_\theta^2\right]^{-1} + \left(1-\vartheta e^{-\delta_t}\right) z\sigma_\epsilon^{-2} \tag{18}$$

and $p_{L,t}$ *is the shadow-price or co-state variable associated with the state variable, and the transversality condition is* $\lim_{t\to\infty}\Omega_{L,t}\beta^t p_{L,t}=0$.

See the Appendix for the proof. This result greatly simplifies the problem by collapsing it to a deterministic dynamic system involving only one state variable, $\Omega_{i,t}$, where $i=H$ or $i=L$. The reason we can do this is that quality $A_{i,t}$ depends on the conditional variance of $\theta_{i,t}$ and because the information structure is similar to that of a Kalman filter, where the sequence of conditional variances is generally deterministic.[7]

[7]The optimal choice of technique is always the same: $a_{i,t}^* = \mathbb{E}_i[\theta_{i,t}|\mathcal{I}_{i,t}]$. The way $a_{i,t}$ enters into expected quality $A_{i,t}$ is through $\mathbb{E}[(\mathbb{E}[\theta_{i,t}|\mathcal{I}_{i,t}]-\theta_{i,t})^2]$, which is the conditional variance $\Omega_{i,t}$. We can replace the entire sequence of $a_{i,t}^*$ with the sequence of variances, which is deterministic here because

This Kalman system has a 2-by-1 observation equation, with $n_{i,t} = z$ signals about $\theta_{i,t}$ and one signal about $\theta_{i,t-1}$. The signal about $\theta_{i,t-1}$ comes from observing last period's output, which reveals quality $A_{i,t-1}$, which, in turn, reveals $\theta_{i,t} + \epsilon_{a,i,t}$.[8]

Equilibrium. From the Hamiltonian functions, and assuming all variances are equal such that $\sigma_\theta^2 = \sigma_a^2 = \sigma_\epsilon^2 = \sigma^2$, we can derive the equilibrium conditions.

$$\frac{\partial H_{H,t}}{\partial \tau_t} = 0 \Rightarrow \beta p_{H,t+1} = \frac{1 - b\overline{A}e^{b\left(\tau_t - \iota\frac{1-m_H}{m_H}\delta_t\right)}}{\vartheta e^{-\left(\tau_t - \iota\frac{1-m_H}{m_H}\delta_t\right)} z\sigma^{-2}} \tag{19}$$

$$\frac{\partial H}{\partial \delta_t} = 0 \Rightarrow \beta p_{H,t+1} = \frac{\pi_t - b\overline{A}\iota e^{b\left(\tau_t - \iota\frac{1-m_H}{m_H}\delta_t\right)}}{\vartheta \iota e^{-\left(\tau_t - \iota\frac{1-m_H}{m_H}\delta_t\right)} z\sigma^{-2}} \tag{20}$$

$$\beta p_{H,t+1} - p_{H,t} = -\frac{\partial H}{\partial \Omega_{H,t}} \Rightarrow \left[\rho + \frac{\sigma^2}{\rho}(\Omega_{H,t} + \sigma^{-2})\right]^{-2} \beta p_{H,t+1} = p_{H,t} - \Omega_{H,t}^{-2} \tag{21}$$

From (32) and (33), it emerges a constant optimal trading price, which is simply $\pi_t = \iota$. The price of protection is directly associated with the degree of its own nonrivalry. If protection is completely non-rival (i.e., $\iota = 0$), then its price is zero; if protection is fully rival, its price is 1.

For the L-type firm, the equilibrium conditions are:

$$\frac{\partial H}{\partial \delta_t} = 0 \Rightarrow \beta p_{L,t+1} = \frac{\pi_t}{\vartheta e^{-\delta_t} z\sigma^{-2}} \tag{22}$$

$$\beta p_{L,t+1} - p_{L,t} = -\frac{\partial H}{\partial \Omega_{L,t}} \Rightarrow \left[\rho + \frac{\sigma^2}{\rho}(\Omega_{L,t} + \sigma^{-2})\right]^{-2} \beta p_{L,t+1} = p_{L,t} - \Omega_{L,t}^{-2} \tag{23}$$

Steady-state. The steady-state of the economy is characterized by a level of cyber security held by H-type firms after trade given by:

$$\tau^* - \iota\frac{1 - m_H}{m_H}\delta^* = -\ln\left(\frac{z - \Xi_H}{\vartheta z}\right) \tag{24}$$

of normality. The only randomness in this model comes from the signals and their realizations, but they never affect the conditional variance, since normal means and variances are independent. Thus, given $\Omega_{i,t-1}$, $\Omega_{i,t}$ is a sufficient statistic for $n_{i,t} = z$ and $\Omega_{i,t+1}$. The mean $\mathbb{E}[\theta_{i,t}|\mathcal{I}_{i,t}]$ is not a state variable because it only matters for determining $a_{i,t}$ and does not affect anything else.

[8]Firms observe $(\theta_{i,t} + \epsilon_{a,i,t})^2$. For tractability, we assume that firms know whether the root is positive or negative. For more on this and for the derivation of the belief updating equations, see online Appendix.

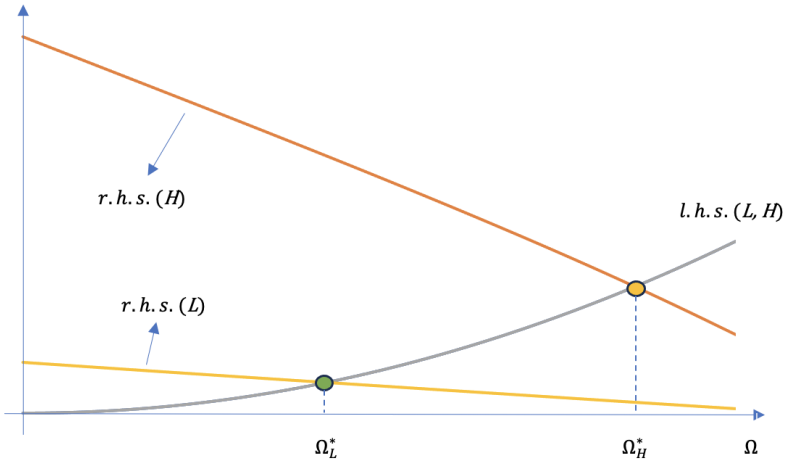
where $\Xi_H \equiv \left\{\Omega_H^* - [\rho^2(\Omega_H^* + \sigma^{-2})^{-1} + \sigma^2]^{-1}\right\}\sigma^2$. At steady-state, the amount of protection bought by L-type firms is given by:

$$\delta^* = -\ln\left(\frac{z - \Xi_L}{\vartheta z}\right) \tag{25}$$

with $\Xi_L \equiv \left\{\Omega_L^* - [\rho^2(\Omega_L^* + \sigma^{-2})^{-1} + \sigma^2]^{-1}\right\}\sigma^2$.

Figure (11) plots the equilibrium knowledge levels of this economy. The demand and supply of knowledge for H-type firms intersect at a higher level than the demand and supply of knowledge for L-type firms. The demand of L-type firms is flatter and more inelastic than the demand of H-type firms. Thus, in equlibrium, H-type firms end up with a higher level of knowledge than L-type firms.

Figure 11: Steady-state stocks of knowledge.



Legend: The figure shows the equilibria levels of knowledge for H-type firms (in orange on the right) and L-type firms (in green on the left) as a function of the cyberrisk index, ϑ, on the X-axis. H-type firms achieve a higher level of steady-state knowledge than L-type firms. The parameters used in this simulations are the following: $z = 10$, $\rho = 0.9$, $\sigma_\theta^2 = \sigma_a^2 = \sigma_\epsilon^2 = \sigma^2 = 2.5$, $m_H = 1/3$, $\iota = 0.6$, $\beta = 0.96$, $\vartheta = 0.75$, $\overline{A} = 25$, $b = 0.035$, and $r = 1$.

Table (14) illustrates the steady state equilibrium of this economy. In the case of this example, in the steady state, H-type firms invest 1.296 in in-house cyber protection, sell 0.130 cyber protection to L-type firms and remain with a cyber protection level of 0.335, which is higher than the L-type's level of protection of 0.130. In steady-state, knowledge, quality and profits are all higher for the H-type firm than for the L-type

firm.

Table 14: Steady-state.

Parameter	**Symbol**	**Steady-state**
Knowledge H-type	$\Omega_H^\star$	3.224
Knowledge L-type	$\Omega_L^\star$	1.609
In-house cyberprotection	$\tau^\star$	1.296
Cybersecurity traded	$\delta^\star$	0.130
Quality H-type	A_H^*	23.207
Quality L-type	A_L^*	21.879
Profits H-type	Π_H^*	21.068
Profits L-type	Π_L^*	20.800
Total output	Y	22.321

Legend: The parameters used in this simulations are the following: $z = 10$, $\rho = 0.9$, $\sigma_\theta^2 = \sigma_a^2 = \sigma_\epsilon^2 = \sigma^2 = 2.5$, $m_H = 1/$
$\vartheta = 0.75$, $\overline{A} = 25$, $b = 0.035$, and $r = 1$.

5.4 Results and implications

Throughout this section, a numerical example is employed with the goal of highlighting some of the most meaningful results of the model. These results comprise the impact of cybercrime over firms' profits, the timing of the decisions to engage in in-house cyber protection and external purchase of cyber security, and aggregate output.

5.4.1 Cyber protection helps firms hedge cyber-risk

Our first numerical experiment studies how an increase in firm cyber risk changes firms' profits. We start by simulating firm profits in a model with no cyber protection. Then, we turn on cyber security protection for both types of firms to observe how their profits change. To compute the change in firms profitability when they face increasingly higher cyber risk, we change the cyber risk index ϑ continuously from no cyber risk ($\vartheta = 0$) to maximum cyber risk ($\vartheta = 1$) and re-compute the steady state. Figure (12) shows that the profits of H-type firms with cyber security fall by less than the profits of L-type firms as cyber risk increases. Moreover, the profits of both types of firms without cyber security protection at all drop dramatically as the overall level of cyber risk increases in the economy.

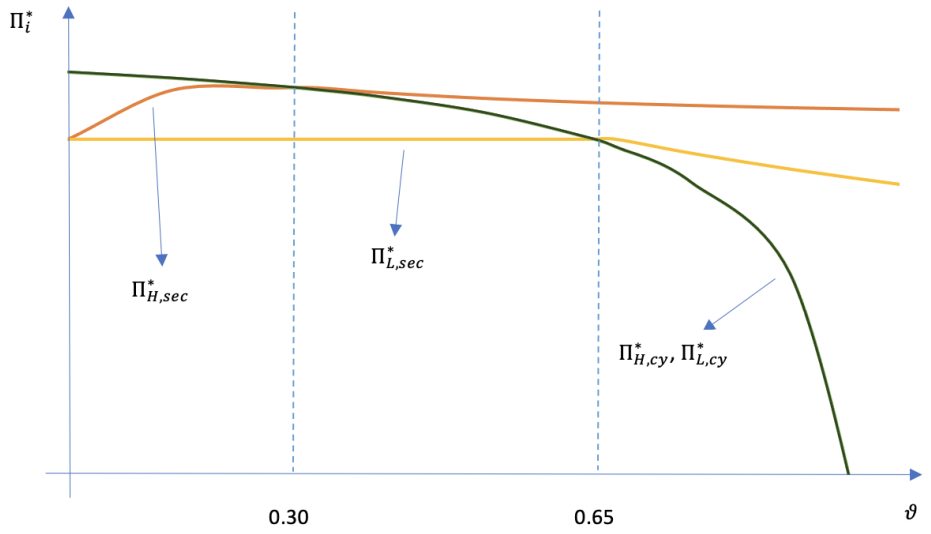
Without protection, the profits (in green) of H-type firms are the same as the profits of L-type firms and decreasing in the cyber risk index ϑ. Initially, the profits without cyber security decline slowly, but after the second threshold, they decline rapidly because the cost incurred in knowledge loss increases exponentially with cyber risk without protection. With protection, however, the profits of H-type firms (in orange) are always higher than the profits of L-type firms (in yellow). And, as cyber risk increases, the profits H-type firms decrease at a smaller rate than the profits of L-type firms (in yellow). An interesting observation is that initially, with protection, the profits of H-type firms first increase because the benefit of protection (which is cyber security-driven innovation) is initially higher than the cost of cyber crime.

5.4.2 High capability firms engage in protection at lower risk levels than L-type firms

What governs the steady-state size of firms is firms' cyber protection levels as a function of the cyberrisk index, ϑ, plotted in Figure (13).

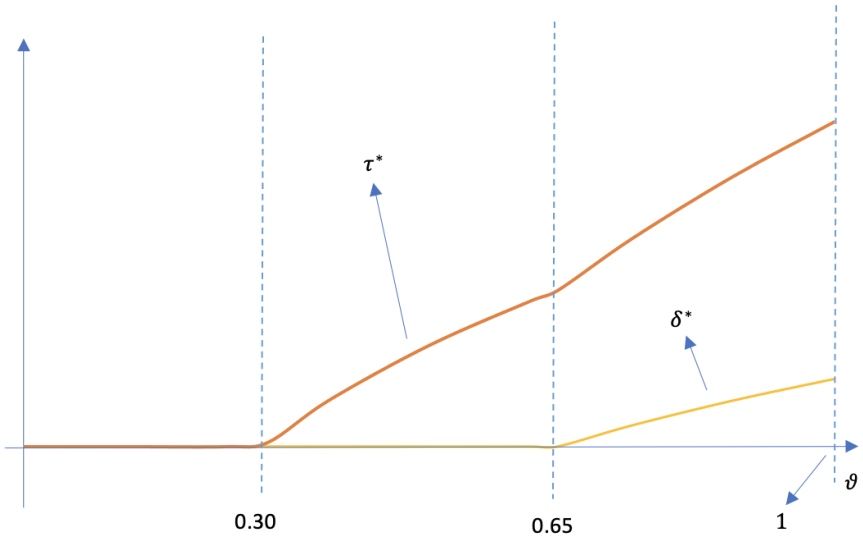
Evaluating the model for different values of ϑ, and letting all other parameters be as

Figure 12: Profits as a function of cyber risk.



Legend: This figure plots the steady-state profit levels for H-type firms with (in orange, $\Pi^{\star}_{H,sec}$) and without cyberprotection (in green, $\Pi^{\star}_{H,cy}$), and L-type firms with (in yellow, $\Pi^{\star}_{L,sec}$) and without cyber protection (in green, $\Pi^{\star}_{L,cy}$), as a function of the cyber risk index, ϑ, on the X-axis. The parameters used in this simulation are the following: the data endowment $z = 10$, the coefficient of the AR(1) process $\rho = 0.9$, all variances $\sigma^2_\theta = \sigma^2_a = \sigma^2_\epsilon = \sigma^2 = 2.5$, the share of H-type firms $m_H = 1/3$, the non-rivalry parameter $\iota = 0.6$, the intertemporal discount factor $\beta = 0.96$, the cyber risk index $\vartheta = 0.75$, the maximum quality threshold $\overline{A} = 25$, the innovation externality $b = 0.035$, and the cost of capital $r = 1$.

Figure 13: Cyberprotection as a function of cyberrisk.



Legend: The figure plots in-house cyber security investment, τ_t, by H-type firms (in orange), and external cyber security acquisition by L-type firms (in yellow). Notice the two critical thresholds at which in-house cyber protection and external cyber protection become strictly positive. The parameters used in this simulations are the following: the data endowment $z = 10$, the coefficient of the AR(1) process $\rho = 0.9$, all variances $\sigma_\theta^2 = \sigma_a^2 = \sigma_\epsilon^2 = \sigma^2 = 2.5$, the share of H-type firms $m_H = 1/3$, the non-rivalry parameter $\iota = 0.6$, the intertemporal discount factor $\beta = 0.96$, the cyber risk index $\vartheta = 0.75$, the maximum quality threshold $\overline{A} = 25$, the innovation externality $b = 0.035$, and the cost of capital $r = 1$.

before, we find two critical thresholds: at $\vartheta = 0.6583$, optimal cyber security purchases, δ^*, changes from negative to positive, implying that L-type firms buy protection only for $\vartheta > 0.6583$. For $\vartheta \leq 0.6583$, H-type firms have to choose whether to invest in protection or not, knowing that they cannot sell any cyber protection. H-type firms are indifferent between investing in protection or not at a critical threhold level of $\vartheta = 0.3$. For $\vartheta > 0.3$, H-type firms invest in protection, otherwise they do not.

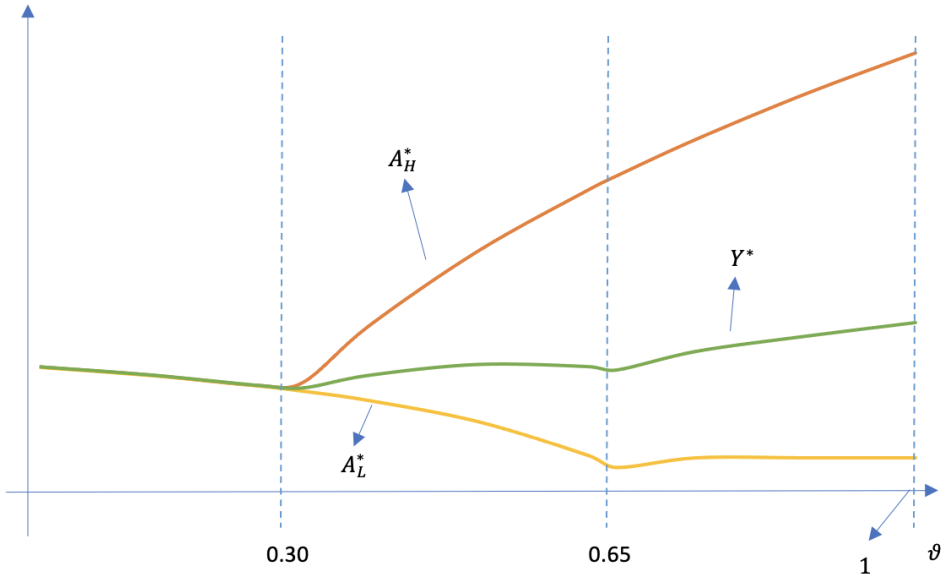
5.4.3 Cyber risk can also sustain growth

Surprisingly, while one expects aggregate economic output to be decreasing in cyber risk, there is a counteracting force that works especially at high levels of risk. This is shown in Figure (14).

Firms with a high capacity for in-house cyber security protection (in orange) use this protection to innovate, which raises the quality and quantity of production. In-

deed, output is increasing in cyber risk for H-type firms at moderate to high levels of cyber risk. L-type firms do not have this positive spillover, because they only use cyber security for their own protection, to mitigate the negative effects of cybercrime. The aggregate output is a weighted average of the output of the two types of firms. Concerning the evolution of Y^* as ϑ increases, one notices that an initial fall is counteracted when H-type firms start to invest in protection, and this process gains momentum when L-type firms start protecting as well.

Figure 14: Output as a function of cyberrisk.

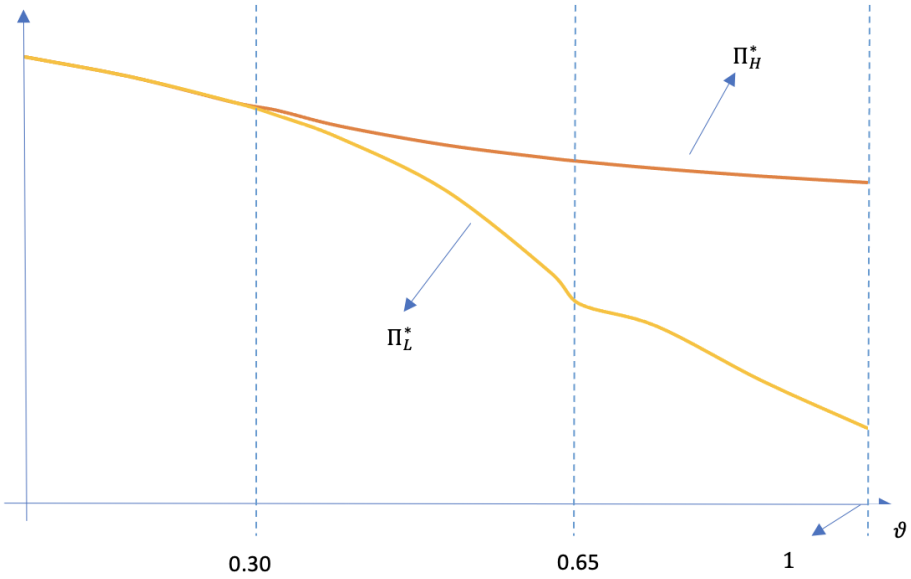


Legend: The parameters used in this simulations are the following: the data endowment $z = 10$, the coefficent of the AR(1) process $\rho = 0.9$, all variances $\sigma_\theta^2 = \sigma_a^2 = \sigma_\epsilon^2 = \sigma^2 = 2.5$, the share of H-type firms $m_H = 1/3$, the non-rivalry parameter $\iota = 0.6$, the intertemporal discount factor $\beta = 0.96$, the cyberrisk index $\vartheta = 0.75$, the maximum quality threshold $\overline{A} = 25$, the innovation externality $b = 0.035$, and the cost of capital $r = 1$.

We can recover the representation of profits in Figure (12), to plot the actual profits, given the choices of firms on whether to get protection or not. Figure (15) clarifies again the existence of three stages and the fact that cybercrime is much less harmful for H-type firms, because these make use of the innovation externality that cybersecurity allows for.

The model is simple, but it generates some powerful predictions. Cyber risk hurts firms in the modern economy and firms make lower profits at increasingly high levels of risk. However, there is a silver lining: cyber risk can sustain growth and innovation

Figure 15: Realized (equilibrium) profits.



Legend: The parameters used in this simulations are the following: the data endowment $z = 10$, the coefficent of the AR(1) process $\rho = 0.9$, all variances $\sigma_\theta^2 = \sigma_a^2 = \sigma_\epsilon^2 = \sigma^2 = 2.5$, the share of H-type firms $m_H = 1/3$, the non-rivalry parameter $\iota = 0.6$, the intertemporal discount factor $\beta = 0.96$, the cyberrisk index $\vartheta = 0.75$, the maximum quality threshold $\overline{A} = 25$, the innovation externality $b = 0.035$, and the cost of capital $r = 1$.

when it allows firms to use cyber security protection for innovation. We allowed some firms in the economy the potential to use cyber security to improve their productivity ceiling. When given this opportunity, cyber risk can sustain firm growth and innovation because there are innovation externalities that arise from cyber risk protection.

6 Conclusion

In this paper, we assess the relationship between cyber risk, cyber security, innovation, and growth. From the empirical stand point, we found evidence that the increased threat of cybercrime and cyber incidents drives innovation in security measures and systems, leading to advancements in technology and potential long-term growth when security measures are developed in-house, in digitally-savvy firm. Essentially, the risk of cybercrime motivates data-intensive companies to actively pursue digital innovation, subsequently enhancing productivity in various aspects of their operations.

In other words, digitally-savvy firms which develop products and services to protect themselves against cyber-risk, benefit from these products and services to improve the quality of their other digital products. In this context, it is noteworthy to consider how Amazon's innovation with the 1-click purchase system relies on a patented innovation that ensures secure data transmission over the internet. This innovation and its associated patent not only revolutionized the online shopping experience but also highlight the critical role of secure data transmission in the digital realm. Amazon's use of their own, internally-developed cyber-security innovation, into their other digital product offerings aligns with our empirical analysis, confirming that digitally-intensive firms respond to cyber risk by boosting their innovation activities with positive spillover effects across multiple product domains.

We also find that early treated firms, in the sense of firms being in states that adopted data breach notification laws early, display the strongest response. This suggests that the nature of cybercrime may have changed over time, becoming more severe and debilitating, increasing firms' costs beyond their ability to invest in innovation to begin with. The exact mechanism for this effect is interesting in itself and the subject of future investigation.

The paper also proposes and discusses the dynamics of a growth model of the data economy where data, crucial for business optimization, is at risk of being damaged and destroyed by cyber criminals or other eventual cyber incidents. We allow firms to protect themselves against cybercrime and even trade cyber security protection. Our simple model features heterogeneity in the type of cyber security a firm invests in. Digitally savvy firms invest in in-house cyber security, which can be used to improve the quality of other products. Non-digitally-savvy firms invest in external cyber security they source from the digitally savvy firms. This external cyber protection they buy is assumed to be not tailored enough for them to be used for the development of other products within those firms.

References

Aghion, Philippe, John Van Reenen, and Luigi Zingales, "Innovation and institutional ownership," *American Economic Review*, 2013, *103* (1), 277–304.

Amore, Mario Daniele, Cedric Schneider, and Alminas Žaldokas, "Credit supply and corporate innovation," *Journal of Financial Economics*, 2013, *109* (3), 835–855.

Anderson, Ross J., Chris J. Barton, Rainer Böhme, Richard Clayton, Michel van Eeten, Michael Levi, Tyler W. Moore, and Stefan Savage, "Measuring the Cost of Cybercrime," in "Workshop on the Economics of Information Security" 2012.

Azoulay, Pierre, Christian Fons-Rosen, and Joshua S Graff Zivin, "Does science advance one funeral at a time?," *American Economic Review*, 2019, *109* (8), 2889–2920.

Babina, Tania, Anastassia Fedyk, Alex Xi He, and James Hodson, "Artificial Intelligence, Firm Growth, and Product Innovation," *Journal of Financial Economics, Forthcoming*, 2023.

Baker, Andrew C., David F. Larcker, and Charles C.Y. Wang, "How much should we trust staggered difference-in-differences estimates?," *Journal of Financial Economics*, 2022, *144* (2), 370–395.

Blundell, Richard, Rachel Griffith, and John Van Reenen, "Market share, market value and innovation in a panel of British manufacturing firms," *The Review of Economic Studies*, 1999, *66* (3), 529–554.

Boasiako, Kwabena A. and Michael O'Connor Keefe, "Data breaches and corporate liquidity management," *European Financial Management*, 2021, *27* (3), 528–551.

Borusyak, Kirill, Xavier Jaravel, and Jann Spiess, "Revisiting Event Study Designs: Robust and Efficient Estimation," Forthcoming in ReStud, 2108.12419, arXiv.org 2022.

Canayaz, Mehmet, Ilja Kantorovitch, and Roxana Mihet, "Consumer Privacy and Value of Consumer Data," Technical Report 22-68 2022.

Cohn, Jonathan B, Zack Liu, and Malcolm I Wardlaw, "Count (and count-like) data in finance," *Journal of Financial Economics*, 2022, *146* (2), 529–551.

Cong, L.W., D. Xie, and L. Zhang, "Knowledge Accumulation, Privacy, and Growth in a Data Economy," *Management Science*, 2021, *67* (10), 6480–6492.

_ , **W. Wei, D. Xie, and L. Zhang**, "Endogenous Growth under Multiple Uses of Data," *Journal of Economic Dynamics and Control*, 2022, *104395.*

Correia, Sergio, Paulo Guimarães, and Tom Zylkin, "Fast Poisson estimation with high-dimensional fixed effects," *The Stata Journal*, 2020, *20* (1), 95–115.

Dass, Nishant, Vikram Nanda, and Steven Chong Xiao, "Truncation bias corrections in patent data: Implications for recent research on innovation," *Journal of Corporate Finance*, 2017, *44*, 353–374.

Ewens, Michael, Ryan Peters, and Sean Wang, "Measuring Intangible Capital with Market Prices," *Working Paper*, 2020.

Farboodi, M. and L. Veldkamp, "A Growth Model of the Data Economy," Technical Report 28427 2021.

Farboodi, Maryam, Roxana Mihet, Thomas Philippon, and Laura Veldkamp, "Big Data and Firm Dynamics," *AER Papers and Proceedings*, May 2019, *109*, 38–42.

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber, "Cybersecurity risk," *The Review of Financial Studies*, 2023, *36* (1), 351–407.

Ganglmair, Bernhard, W Keith Robinson, and Michael Seeligson, "The rise of process claims: Evidence from a century of US patents," *Available at SSRN 4069994*, 2022.

Giczy, Alexander V, Nicholas A Pairolero, and Andrew A Toole, "Identifying artificial intelligence (AI) invention: A novel AI patent dataset," *The Journal of Technology Transfer*, 2022, *47* (2), 476–505.

Goodman-Bacon, Andrew, "Difference-in-differences with variation in treatment timing," *Journal of Econometrics*, 2021, *225* (2), 254–277.

Hall, Bronwyn H, Adam B Jaffe, and Manuel Trajtenberg, "The NBER patent citation data file: Lessons, insights and methodological tools," 2001.

_ , **Adam Jaffe, and Manuel Trajtenberg**, "Market value and patent citations," *RAND Journal of economics*, 2005, pp. 16–38.

Hausman, Jerry, Bronwyn H. Hall, and Zvi Griliches, "Econometric Models for Count Data with an Application to the Patents-R & D Relationship," *Econometrica*, 1984, *52* (4), 909–938.

Hoberg, Gerard and Gordon Phillips, "Text-based network industries and endogenous product differentiation," *Journal of Political Economy*, 2016, *124* (5), 1423–1465.

Hou, Y., J. Huang, D. Xie, and W. Zhou, "The Limits to Growth in the Data Economy: How Data Storage Constraint Threats," Technical Report 4099544 2022.

Howell, Sabrina T, "Financing innovation: Evidence from R&D grants," *American Economic Review*, 2017, *107* (4), 1136–64.

Huang, Henry and Chong Wang, "Do Banks Price Firms' Data Breaches?," *The Accounting Review*, 2021, *96* (3), 261–286.

Jamilov, Rustam, Hélène Rey, and Ahmed Tahoun, "The anatomy of cyber risk," Technical Report, National Bureau of Economic Research 2021.

_ , Hélène Rey, and Ahmed Tahoun, "The Anatomy of Cyber Risk," Working Paper 28906, National Bureau of Economic Research June 2021.

Jones, C.I. and C. Tonetti, "Nonrivalry and the Economics of Data," *American Economic Review*, 2020, *110* (9), 2819–2858.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms," *Journal of Financial Economics*, 2021, *139* (3), 719–749.

Kogan, Leonid, Dimitris Papanikolaou, Amit Seru, and Noah Stoffman, "Technological innovation, resource allocation, and growth," *The Quarterly Journal of Economics*, 2017, *132* (2), 665–712.

Lattanzio, Gabriele and Yue Ma, "Cybersecurity risk and corporate innovation," *Journal of Corporate Finance*, 2023, p. 102445.

Lerner, Josh and Amit Seru, "The use and misuse of patent data: Issues for finance and beyond," *The Review of Financial Studies*, 2022, *35* (6), 2667–2704.

Liu, Jinyu and Xiaoran Ni, "Ordeal by innocence in the big-data era: Intended data breach disclosure, unintended real activities manipulation," *European Financial Management*, 2023.

Murciano-Goroff, Raviv, "Do Data Breach Disclosure Laws Increase Firms' Investment in Securing Their Digital Infrastructure?," in "in."

Silva, JMC Santos and Silvana Tenreyro, "The log of gravity," *The Review of Economics and statistics*, 2006, *88* (4), 641–658.

_ and _ , "Further simulation evidence on the performance of the Poisson pseudo-maximum likelihood estimator," *Economics Letters*, 2011, *112* (2), 220–222.

Wooldridge, Jeffrey M, "Distribution-free estimation of some nonlinear panel data models," *Journal of Econometrics*, 1999, *90* (1), 77–97.

[12pt,letter]article

[left=3cm, right=3cm, top=3cm, bottom=3cm]geometry

setspace,amsfonts,comment,amsmath,amssymb,amsxtra,ushort,tikz,graphicx,pgfplots,units,xfrac hyperref lscape afterpage natbib setspace graphicx [caption]subfig setspace amsmath kantlipsum [title]appendix longtable longtable,threeparttablex setspace comment

Online Appendix

Appendix A Theoretical derivations

A.1 Model Solution Details

There are two sources of uncertainty in firm i's problem at date t: the (random) optimal technique $\theta_{i,t}$, and the aggregate price P_t. Let $(\hat{\mu}_{i,t}, \Omega_{i,t})$ denote the conditional mean and precision of firm i belief about $\theta_{i,t}$ given its information set at date t, $\mathcal{I}_{i,t}$.

In this section, we will first describe the firm belief updating process about its optimal technique. Next, we argue that in this environment, the firm's optimal production choice is deterministic, and thus the price is deterministic as well. Finally, we lay out the full set of equations that characterize the equilibrium of this economy with two groups of firms.

Belief updating The information problem of firm i about its optimal technique $\theta_{i,t}$ can be expressed as a Kalman filtering system, with a 2-by-1 observation equation, $(\hat{\mu}_{i,t}, \Omega_{i,t})$.

We start by describing the Kalman system, and show that the sequence of conditional variances is deterministic. Note that all the variables are firm specific, but since the information problem is solved firm-by-firm, for brevity we suppress the dependence on firm index i.

At time t, each firm observes two types of signals. First, date $t-1$ output provides a noisy signal about θ_{t-1}:

$$y_{t-1} = \theta_{t-1} + \epsilon_{a,t-1}, \tag{26}$$

where $\epsilon_{a,t} \sim \mathcal{N}(0, \sigma_a^2)$. We provide model detail on this step below. Second, the firm observes $n_t = z_t$ data points as a bi-product of its economic activity. The set of signals

$\{s_{t,m}\}_{m\in[1:n_{i,t}]}$ are equivalent to an aggregate (average) signal $\bar{s}_t$ such that:

$$\bar{s}_t = \theta_t + \epsilon_{s,t}, \tag{27}$$

where $\epsilon_{s,t} \sim \mathcal{N}(0, \sigma_\epsilon^2/n_t)$. The state equation is

$$\theta_t - \bar{\theta} = \rho(\theta_{t-1} - \bar{\theta}) + \eta_t,$$

where $\eta_t \sim \mathcal{N}(0, \sigma_\theta^2)$.

At time, t, the firm takes as given:

$$\begin{aligned}\widehat{\mu}_{t-1} &= \mathbb{E}\left[\theta_t \mid s^{t-1}, y^{t-2}\right] \\ \Omega_{t-1}^{-1} &= Var\left[\theta_t \mid s^{t-1}, y^{t-2}\right]\end{aligned}$$

where $s^{t-1} = \{s_{t-1}, s_{t-2}, \dots\}$ and $y^{t-2} = \{y_{t-2}, y_{it-3}, \dots\}$ denote the histories of the observed variables, and $s_t = \{s_{t,m}\}_{m\in[1:n_{i,t}]}$.

We update the state variable sequentially, using the two signals. First, combine the priors with y_{t-1}:

$$\begin{aligned}\mathbb{E}\left[\theta_{t-1} \mid \mathcal{I}_{t-1}, y_{t-1}\right] &= \frac{\Omega_{t-1}\widehat{\mu}_{t-1} + \sigma_a^{-2} y_{t-1}}{\Omega_{t-1} + \sigma_a^{-2}} \\ V\left[\theta_{t-1} \mid \mathcal{I}_{t-1}, y_{t-1}\right] &= \left[\Omega_{t-1} + \sigma_a^{-2}\right]^{-1} \\ \mathbb{E}\left[\theta_t \mid \mathcal{I}_{t-1}, y_{t-1}\right] &= \bar{\theta} + \rho \cdot \left(\mathbb{E}\left[\theta_{t-1} \mid \mathcal{I}_{t-1}, y_{t-1}\right] - \bar{\theta}\right) \\ V\left[\theta_t \mid \mathcal{I}_{t-1}, y_{t-1}\right] &= \rho^2\left[\Omega_{t-1} + \sigma_a^{-2}\right]^{-1} + \sigma_\theta^2\end{aligned}$$

Then, use these as priors and update them with $\bar{s}_t$:

$$\widehat{\mu}_t = \mathbb{E}\left[\theta_t \mid \mathcal{I}_t\right] = \frac{\left[\rho^2\left[\Omega_{t-1} + \sigma_a^{-2}\right]^{-1} + \sigma_\theta^2\right]^{-1} \cdot \mathbb{E}\left[\theta_t \mid \mathcal{I}_{t-1}, y_{t-1}\right] + n_t\sigma_\epsilon^{-2}\bar{s}_t}{\left[\rho^2\left[\Omega_{t-1} + \sigma_a^{-2}\right]^{-1} + \sigma_\theta^2\right]^{-1} + n_t\sigma_\epsilon^{-2}} \tag{28}$$

$$\Omega_t^{-1} = Var\left[\theta \mid \mathcal{I}_t\right] = \left\{\left[\rho^2\left[\Omega_{t-1} + \sigma_a^{-2}\right]^{-1} + \sigma_\theta^2\right]^{-1} + n_t\sigma_\epsilon^{-2}\right\}^{-1} \tag{29}$$

Multiply and divide equation (28) by Ω_t^{-1} as defined in equation (29) to get

$$\widehat{\mu}_t = (1 - n_t\sigma_\epsilon^{-2}\Omega_t^{-1})\left[\bar{\theta}(1-\rho) + \rho\left((1-M_t)\mu_{t-1} + M_t\tilde{y}_{t-1}\right)\right] + n_t\sigma_\epsilon^{-2}\Omega_t^{-1}\bar{s}_t, \tag{30}$$

where $M_t = \sigma_a^{-2}(\Sigma_{t-1} + \sigma_a^{-2})^{-1}$.

Equations (29) and (30) constitute the Kalman filter describing the firm dynamic information problem. Importantly, note that Ω_t^{-1} is deterministic.

Appendix B Modeling quadratic-normal signals from output

When y_{t-1} is observed, agents can back out A_{t-1} exactly. To keep the model simple, we assumed that when agents see A_{t-1}, they also learn whether the quadratic term $(a_{t-1} - \theta_{t-1} - \epsilon_{a,t-1})^2$ had a positive or negative root. An interpretation is that they can figure out if their action a_t was too high or too low.

Relaxing this assumption complicates the model because, when agents do not know which root of the square was realized, the signal is no longer normal. One might solve a model with binomial distribution over two normal variables, perhaps with other simplifying assumptions. For numerical work, a good approximate solution would be to simulate the binomial-normal and then allows firms to observe a normal signal with the same mean and same variance as the true binomial-normal signal. This would capture the right amount of information flow, and keep the tractability of updating with normal variables.

Appendix C The cybersecurity planning problems: optimality conditions and steady state results

C.1 H-type firm

The current-value Hamiltonian function for the H-type firm:

$$H(\Omega_{H,t}; \tau_t; \delta_t; p_{H,t}) = \Pi_{H,t,\text{sec}}$$
$$+\beta p_{H,t+1} \left\{ \left[\rho^2(\Omega_{H,t} + \sigma^{-2})^{-1} + \sigma^2\right]^{-1} + \left[1 - \vartheta e^{-\left(\tau_t - \iota \frac{1-u}{u}\delta_t\right)}\right] z\sigma^{-2} - \Omega_{i,t} \right\} \tag{31}$$

where $p_{H,t}$ is the shadow-price or co-state variable associated with the state vari-

able. The transversality condition is $\lim_{t\to\infty}\Omega_{H,t}\beta^t p_{H,t}=0$.

The first-order optimality conditions:

$$\frac{\partial H}{\partial \tau_t}=0\Rightarrow \beta p_{H,t+1}=\frac{1-b\overline{A}e^{b\left(\tau_t-\iota\frac{1-u}{u}\delta_t\right)}}{\vartheta e^{-\left(\tau_t-\iota\frac{1-u}{u}\delta_t\right)}z\sigma^{-2}} \tag{32}$$

$$\frac{\partial H}{\partial \delta_t}=0\Rightarrow \beta p_{H,t+1}=\frac{\pi_t-b\overline{A}\iota e^{b\left(\tau_t-\iota\frac{1-u}{u}\delta_t\right)}}{\vartheta\iota e^{-\left(\tau_t-\iota\frac{1-u}{u}\delta_t\right)}z\sigma^{-2}} \tag{33}$$

$$\beta p_{H,t+1}-p_{H,t}=-\frac{\partial H}{\partial \Omega_{H,t}}\Rightarrow\left[\rho+\frac{\sigma^2}{\rho}(\Omega_{H,t}+\sigma^{-2})\right]^{-2}\beta p_{H,t+1}=p_{H,t}-\Omega_{H,t}^{-2} \tag{34}$$

From (32) and (33), it emerges a constant optimal trading price, which is simply $\pi_t=\iota$. The price of protection is directly associated with the degree of its own nonrivalry. If protection is completely non-rival (i.e., $\iota=0$), then its price is zero; if protection is fully rival, its price is 1.

Replacing (32) into (34), and evaluating in the steady state, one gets:

$$\Gamma_H=\frac{\vartheta z e^{-\left(\tau^*-\iota\frac{1-u}{u}\delta^*\right)}}{1-b\overline{A}e^{b\left(\tau^*-\iota\frac{1-u}{u}\delta^*\right)}}, \tag{35}$$

with Γ_H defined as $\Gamma_H\equiv\left\{\frac{1}{\beta}-\left[\rho+\frac{\sigma^2}{\rho}(\Omega_H^*+\sigma^{-2})\right]^{-2}\right\}(\Omega_H^*)^2\sigma^2$.

Given constraint (16), it is also true, for the H-firms:

$$\Xi_H=\left[1-\vartheta e^{-\left(\tau^*-\iota\frac{1-u}{u}\delta^*\right)}\right]z, \tag{36}$$

with $\Xi_H\equiv\left\{\Omega_H^*-[\rho^2(\Omega_H^*+\sigma^{-2})^{-1}+\sigma^2]^{-1}\right\}\sigma^2$.

Combining expressions (35) and (36), one obtains a steady state relation that allows for the derivation of Ω_H^*:

$$\Gamma_H=\frac{z-\Xi_H}{1-b\overline{A}\left(\frac{\vartheta z}{z-\Xi_H}\right)^b} \tag{37}$$

Γ_H is such that if $\Omega_H^*=0$ then $\Gamma_H=0$ and if $\Omega_H^*\to+\infty$ then $\Gamma_H\to+\infty$.

Ξ_H is such that if $\Omega_H^*=0$ then $\Xi_H=-\frac{1}{1+\rho^2}$ and if $\Omega_H^*\to+\infty$ then $\Xi_H\to+\infty$. Hence, if $\Omega_H^*=0$ then $\frac{z-\Xi_H}{1-b\overline{A}\left(\frac{\vartheta z}{z-\Xi_H}\right)^b}=\frac{z+\frac{1}{1+\rho^2}}{1-b\overline{A}\left(\frac{\vartheta z}{z+\frac{1}{1+\rho^2}}\right)^b}$; this is a positive value for

$b\overline{A}\left(\frac{\vartheta z}{z+\frac{1}{1+\rho^2}}\right)^b < 1$. If $\Omega_H^* \to +\infty$ then $\frac{z-\Xi_H}{1-b\overline{A}\left(\frac{\vartheta z}{z-\Xi_H}\right)^b} \to -\infty$.

By combining the above reasoning, as long as $b\overline{A}\left(\frac{\vartheta z}{z+\frac{1}{1+\rho^2}}\right)^b < 1$, the l.h.s. of (37) (positively sloped) will intersect the r.h.s. of (37) (negatively sloped) at one single point, and therefore a unique Ω_H^* is derived.

Thus, condition $b\overline{A}\left(\frac{\vartheta z}{z+\frac{1}{1+\rho^2}}\right)^b < 1$ must hold, which can be rewritten as a constraint on ϑ: $\vartheta < \frac{z+\frac{1}{1+\rho^2}}{z}\left(b\overline{A}\right)^{-1/b}$. Because $\vartheta \leq 1$, this constraint is always satisfied as long as $b\overline{A} < 1$.

From (36) also note that the value of security that firm H holds after trade is also a unique constant value,

$$\tau^* - \iota\frac{1-u}{u}\delta^* = -\ln\left(\frac{z-\Xi_H}{\vartheta z}\right) \tag{38}$$

C.2 L-type firm

Turning to the L-type firm, the current-value Hamiltonian is:

$$\begin{aligned} H(\Omega_{L,t};\delta_t;p_{L,t}) &= \Pi_{L,t,\text{sec}} \\ +\beta p_{L,t+1}\left\{\left[\rho^2(\Omega_{L,t}+\sigma^{-2})^{-1}+\sigma^2\right]^{-1} + \left(1-\vartheta e^{-\delta_t}\right)z\sigma^{-2} - \Omega_{i,t}\right\} \end{aligned} \tag{39}$$

The transversality condition: $\lim_{t\to\infty}\Omega_{L,t}\beta^t p_{L,t} = 0$.

The first-order conditions are:

$$\frac{\partial H}{\partial \delta_t} = 0 \Rightarrow \beta p_{L,t+1} = \frac{\pi_t}{\vartheta e^{-\delta_t} z\sigma^{-2}} \tag{40}$$

$$\beta p_{L,t+1} - p_{L,t} = -\frac{\partial H}{\partial \Omega_{L,t}} \Rightarrow \left[\rho + \frac{\sigma^2}{\rho}(\Omega_{L,t}+\sigma^{-2})\right]^{-2}\beta p_{L,t+1} = p_{L,t} - \Omega_{L,t}^{-2} \tag{41}$$

Replace (40) into (41), and recall that we already know that $\pi_t = \iota$. With this information, the following steady state condition holds:

$$\Gamma_L = \vartheta z e^{-\delta^*}, \tag{42}$$

with $\Gamma_L \equiv \left\{\frac{1}{\beta} - \left[\rho + \frac{\sigma^2}{\rho}(\Omega_L^* + \sigma^{-2})\right]^{-2}\right\}(\Omega_L^*)^2\,\sigma^2$.

Given constraint (18),

$$\Xi_L = \left(1 - \vartheta e^{-\delta^*}\right) z, \tag{43}$$

with $\Xi_L \equiv \left\{\Omega_L^* - [\rho^2(\Omega_L^* + \sigma^{-2})^{-1} + \sigma^2]^{-1}\right\} \sigma^2$.

From (42) and (43), a simple expression emerges for the determination of Ω_L^*,

$$\Gamma_L = z - \Xi_L \tag{44}$$

Equation (44) allows for the derivation of a unique Ω_L^*, because the l.h.s. of the expression is a continuous increasing function starting at zero and diverging to infinity (as Ω_L increases) and the l.h.s. is a continuous decreasing function starting at a positive value and falling to minus infinity (as Ω_L increases).

From (43), one can also compute the steady state value of the amount of security bought by firm L:

$$\delta^* = -\ln\left(\frac{z - \Xi_L}{\vartheta z}\right) \tag{45}$$

A unique δ^* exists as well.

By now, we have computed all the relevant steady state values: Ω_H^* and Ω_L^*, and also δ^* (determined from the L-firm problem), and τ^*, determined from (38) after knowing δ^* (the H-type only decides how much to invest in cyberprotection after knowing how much protection firms in the L sector are willing to buy at price $\pi_t = \iota$).

C.3 Steady-state

Possible steady state scenarios:

- (i) The cybersecurity optimal result is such that $\tau^* \leq 0$: firms H do not invest in cybersecurity $\tau^* = 0$ and firms L have no cyberprotection to buy, $\delta^* = 0$. Firms face the problem with no security and their profits are: $\Pi_{H,cy}^* = \Pi_{L,cy}^*$.

- (ii) The cybersecurity optimal result is such that $\tau^* > 0$, $\delta^* \leq 0$: firms L will not buy any protection and face the no-protection problem, with profits $\Pi_{L,cy}^*$. Firms of the H type have two possibilities: to invest τ^*, even though they cannot optimally exchange protection, or not to invest; they compare profits $\Pi_{H,\text{sec}}^*$ and $\Pi_{H,cy}^*$ and choose the option that delivers the highest profits.

- (iii) The cybersecurity optimal result is such that $\tau^* > 0$ and $\delta^* > 0$: firms find it optimal to invest a positive value in cybersecurity (H) and to trade a positive

amount of cybersecurity. In this case, the best option is the cybesecurity one with profits $\Pi^*_{H,\text{sec}}$ and $\Pi^*_{L,\text{sec}}$

Note that conditions $\tau^* > 0$ and $\delta^* > 0$ impose relevant constraints on parameter values, namely, in the first case, $z > \Xi_H$ and $\vartheta > \frac{z-\Xi_H}{z}$ and, in the second case, $z > \Xi_L$ and $\vartheta > \frac{z-\Xi_L}{z}$. These results suggest that investment and trading in cybersecurity require the cybercrime index ϑ to be above a given threshold.

C.4 Comparative statics

A few intuitive comparative statics outcomes (in the cybersecurity setting, i.e., for $\tau^* > 0$, $\delta^* > 0$):

- (i) $\Delta z > 0$: l.h.s. of (37) does not shift; r.h.s. of (37) shifts right $\Rightarrow$ higher Ω^*_H / l.h.s. of (44) does not move; r.h.s. of (44) shifts right $\Rightarrow$ higher Ω^*_L / δ^* and τ^* increase / output of both types of firms will increase.

- (ii) $\Delta u > 0$: Ω^*_H, Ω^*_L, and δ^* do not change; only τ^* decreases - logical result: relatively more firms investing in cyberprotection implies lower investment by each of them to attain the optimal result. Output of L firms is maintained; output of H firms is also maintained (the decrease in τ^* is compensated by the increase in u and, according to (38), there is no change on the available protection and, thus, on output).

- (iii) $\Delta \iota > 0$: Ω^*_H, Ω^*_L, and δ^* do not change; only τ^* decreases - logical result: a lower degree of non-rivalry in selling protection implies H firms will invest more to keep more protection and to profit more from trading. Output does not change for any of the firms for reasons similar to those of the previous item.

- (iv) $\Delta \vartheta > 0$: l.h.s. of (37) does not shift; r.h.s. of (37) shifts right $\Rightarrow$ higher Ω^*_H (this is the positive effect that innovation from cybersecurity has over knowledge when H firms increase cybersecurity in response to cybercrime) / Ω^*_L remains unchanged / δ^* increases (L firms demand more security to face higher risks) / τ^* increases due to the increase on δ^* and directly on ϑ. Output levels will increase, given the corresponding expressions.

- (v) $\Delta b > 0$: l.h.s. of (37) does not shift; r.h.s. of (37) shifts right $\Rightarrow$ higher Ω^*_H / Ω^*_L remains unchanged / τ^* increases because of the increase in Ω^*_H; δ^* does not change / the output of L firms does not change / the output of H firms increases.

Appendix D Simulating the data economy: a numerical example

Take the values in Table 1.

Parameter	Symbol	Value
Data endowment	z	10
Coefficent of the AR(1) process	ρ	0.9
Variances	σ^2	2.5
Share of H-type firms	u	1/3
Non-rivalry parameter	ι	0.6
Intertemporal discount factor	β	0.96
Cyberrisk index	ϑ	0.75
Maximum quality	$\overline{A}$	25
Inonvation externality	b	0.035
Capital cost	r	1

TABLE 1 - VALUES OF PARAMETERS.

For these values of parameters: $\Omega_H^* = 3.224$ and $\Omega_L^* = 1.609$. These results are found in the intersection of the l.h.s. and r.h.s. of (37) and (44) [**Fig.1**]

Applying the corresponding formulas, $\delta^* = 0.130$ and $\tau^* = 1.296$ (these are both positive values and, therefore, firms engage in cybersecurity investment and cybersecurity trading).

Replacing the equilibrium values in the expressions for output and profits, $A_H^* = 23.207$ and $A_L^* = 21.879$ ($A_H^* > A_L^*$); $\Pi_{H,\text{sec}}^* = 21.068$ and $\Pi_{L,\text{sec}}^* = 20.800$ ($\Pi_{H,\text{sec}}^* > \Pi_{L,\text{sec}}^*$). Also, $Y^* = uA_H^* + (1-u)A_L^* = 22.321$.

D.1 Comparative statics

How do steady state values change with cyberrisk?

Recall that $\vartheta \in [0,1]$. Evaluating the model for different values of ϑ (and letting all other values be as in Table 1), we find two thresholds: at $\vartheta = \frac{z-\Xi_L}{z} = 0.6583$, optimal security purchasing, δ^*, changes from negative to positive, implying that firms L buy protection only for $\vartheta > 0.6583$. For $\vartheta \leq 0.6583$, H firms have to choose whether to invest in protection or not, knowing that they will sell no protection. They compare

profits $\Pi^*_{H,\text{sec}}$ and $\Pi^*_{H,cy}$; these are equal around $\vartheta = 0.3$. For $\vartheta > 0.3$, H-type firms invest in protection, otherwise they do not.

Fig.2 draws profits without protection for both firms (these are identical), the profits of the H firms with security investment, and the profits of the L firms under security trading. The two mentioned thresholds are highlighted.

Hence: for $\vartheta \leq 0.3$, H-firms do not invest in cyberprotection and L-firms do not buy protection; for $0.3 < \vartheta \leq 0.6583$, H firms invest in protection and L firms buy no protection; for $\vartheta > 0.6583$, H-type firms invest in protection and L-type firms buy protection. In this last segment, the higher the value of ϑ, the more the H firms invest and the more L firms buy.

Fig. 3 presents the investment and trading levels. Again, the two thresholds are clear (notice the second jump in τ^*; this occurs because to the right of that point, H-type firms need to invest in security for their one use but also to sell to firms in the L group).

Fig. 4: output of each type of firm and aggregate output, for different levels of cyberrisk. In the first segment, the output is the same (the firms are identical); in the second segment, L firms face increasing risk but do not protect and, consequently, output falls (because the stock of knowledge falls); H firms start investing in cybersecurity what has the innovation side effect and, therefore, they are able to increase output. In the third segment, H firms continue to invest in cyberprotection and innovate; L firms start purchasing security that they cannot use to innovate but that prevents output from falling (i.e., it allows to maintain the stock of knowledge as the cyberrisk increases).

The aggregate output is a weighted average of the output of the two types of firms (recall that, in the example, L firms are two thirds of the total number of firms). Concerning the evolution of Y^* as ϑ increases, one notices that an initial fall is counteracted when H firms start to invest in protection, and this process gains a new impetus when L firms start protecting as well.

We can recover the representation of profits in Fig.2, to draw the actual profits, given the choices of firms on whether to get protection or not. **Fig. 5** clarifies again the existence of three stages and the fact that cybercrime is much less harmful for H-type firms, because these make use of the innovation externality that cybersecurity allows for.

D.2 Does data growth cause economic growth?

In the model, there are various parameters whose values can change - $\vartheta, \iota, u, b, ...$ - but only one can grow in a sustained way over time, which is the endowment of data, z. The question is: if one makes z to increase over time at a constant rate, will the economy's output also grow over time at a constant rate?

The answer is no: simulations show that although the increase in z leads to increases in Ω_H^* and Ω_L^*, they also lead to falls in δ^* and τ^* (more data and a same cyberrisk lead to the need of less protection). For large values of z, τ^* becomes zero, and without investment in cybersecurity there is no cyberrisk induced innovation and the maximum quality of output cannot expand. The increases in Ω_H^* and Ω_L^* are associated with decreasing marginal returns and, therefore, although z might grow in a sustained way, this is not accompanied by an increase in the firms' output.