The Impact of Ransomware Attacks on Security Portfolios: Firm-Level Panel Data

Abulfaz Hajizada, Dana Etgar Itzhaki, Noa Barnir, Tyler Moore, Neil Gandal

April 27, 2026

Abstract

We study how firms adjust their cybersecurity postures after experiencing a cyber attack. We combine publicly disclosed ransomware cyber incidents with detailed data on security products and vendor deployments from the Spiceworks Ziff Davis (SWZD) Company Intelligence Database (CIDB) over multiple years. Our empirical approach compares attacked firms to similar non-attacked firms using econometrics and employing a difference-in-difference (DID) framework.

Controlling for common changes made by all firms over time, we find that "attacked" firms increased the breadth of their security posture relative to non-attacked firms. They adopted more National Institute of Standards and Technology (NIST) functions and had broader "category coverage" than non-attacked firms in the "post attack" period. Attacked firms also increased the usage of security products from large and "platform" vendors relative to non-attacked firms in the "post attack" period.[1]

[1]Gandal and Moore gratefully acknowledge support from the US National Science Foundation (NSF) Award No. 2147505 and Award No. 2452738 and the US Israel Binational Science Foundation (BSF) Award No. 2016622 and Award No. 2021711. Hajizada and Moore: University of Tulsa; Itzhaki and Barnir: Tel Aviv University; Gandal: Tel Aviv University and University of Tulsa

1 Introduction

Cyber attacks are becoming more frequent and more sophisticated, creating growing challenges for firms. In response, organizations invest heavily in cybersecurity and deploy an increasing number of security products and services. While there is broad agreement that cybersecurity investment has increased over time, there is limited empirical evidence on how firms adjust their cybersecurity strategies after experiencing a cyber attack. Aggregate investment levels provide an incomplete picture of firm level cybersecurity posture especially in response to cyber attacks. Hence, it remains unclear whether attacks lead firms only to increase the overall level of investment, or whether they also change how investments are allocated across security products and vendors.

In this paper, we study how firms adjust their cybersecurity products and vendor portfolios after experiencing a cyber attack. We use data from the Spiceworks Ziff Davis (SWZD) Company Intelligence Database (CIDB) [12], which tracks IT and security product installations by firm and vendor, combined with a dataset of publicly disclosed ransomware cyber attacks in 2019 or 2020 from Temple University [9].

The CIDB database has detailed information on firms and the technologies. This dataset reports over 11,000 IT infrastructure products at the firm/site level for the years 2018, 2020, and 2022. The CIDB comprises 90% of Information Technology (IT) purchases in the world. In particular, the CIDB has the following which are important for the analysis:

- *"Firmographics"*: demographic attributes of firms such as industry sector, number of employees and geographic location.
- *IT Security "Technographics"*: information on each IT security product and service utilized by industries and firms.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) recommends that all organizations adopt a baseline set of products that cover the following five "functions": Identify, Protect, Defend, Respond, and Recover [8][2] Our data enables us to examine what happens when firms are attacked. Do they increase the breadth" of their security posture in the "post attack" period? We measure breadth as follows:

- The total number of (the five) NIST functions covered by the firm.
- The number of CIDB "security categories" covered by the firm. There are twelve such categories. We explicitly discuss these categories below.

Hence, we classify security products according to two "breadth" metrics (i) NIST functions and (ii) CIDB categories. We also examine the "total number of security products" employed by the firms; this measures "depth", rather than breadth, since firms can have several different products in a particular CIDB category.

[2]A brief description of the five functions can be found at https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions.

1.1 Summary of our methodology and results

We employ data from the CIDB for 2018 and 2022 in order to observe changes in firms' cybersecurity posture before and after attacks. While we have data from 2018, 2020, and 2022, we do not always know the exact date of the attack, just the year (2019 or 2020). We also do not know whether the CIDB data are from the beginning of the year, the end of the year, or at another point in time[3]. Hence, it makes sense to use the 2018 data as the "before the attack" period and the 2022 data as the "after attack period."

The CIDB product data are delineated in "product series". Three of the twenty-four CIDB product series are specific to security: *Security Devices*, *IT Security Information*, and *Network Security Monitoring*. We focus on these three product series.

In all, there are 507 security products in the three CIDB security product series. The CIDB classifies all the 507 security products into twelve CIDB security categories. See Table 1.[4] We then map these categories into five functional categories defined by the National Institute of Standards and Technology (NIST): Identify, Protect, Detect, Respond, and Recover [8].

For the analysis, we use publicly traded US firms from the Temple Critical Infrastructure Ransomware Attacks (CIRA) dataset [9]. Publicly traded firms in the US are required to disclose cyber risks and cyber attacks. The CIRA data has 102 US firms that publicly disclosed attacks in 2019 and 2020 (36 in 2019 and 68 in 2020).

To construct a comparison group, we match each attacked firm to a non-attacked firm in the 2018 CIDB dataset by using the Standard Industrial Classification (SIC) codes that indicate the company's type of business. We use the SIC four digit codes (SIC4); hence the industry delineation is quite detailed. We then match by firm size (employee count).

Our empirical strategy compares firms that experienced a cyber attack in 2019 or 2020 to matched firms that did not experience an attack. We use a difference-in-differences framework to control for common time trends (and "pre-attack" security posture) in cybersecurity adoption. This approach allows us to isolate how attacked firms adjust their cybersecurity posture relative to similarly non-attacked firms.

We document two main findings. First, although cybersecurity coverage increased over time for all firms, regardless of whether they experienced a cyber attack, attacked firms increased the breadth of their security posture relative to non-attacked firms.

By breadth, we mean that they adopted more NIST functions and added more CIDB "category" coverage[5] than non-attacked firms in the "post attack" period and the difference is statistically significant. We show that these patterns are especially pronounced in the case of four core CIDB security categories: Firewall, Identity and Access Management, Endpoint Security, and Security Information and Event Management (SIEM).[6]

Second, we find that cyber attacks are also associated with changes in vendor portfolios. Compared to non-attacked firms, attacked firms were more likely to shift to vendors with

[3]Formally, the CIDB measures are based on a snapshot taken on December 31 of the year in question. However, the process of updating each company's entries can occur throughout the year, hence the granularity of the data can be best interpreted at the yearly level.

[4]Compared to enterprise IT products, security products have been categorized much more systematically.

[5]See Table 1 for the five NIST Functions and the twelve CIDB categories.

[6]These measures are more important than the total number of security products, since security products may include duplicate products in a category, i.e., several firewalls.

larger market presence and broader product scope.

The remainder of the paper is organized as follows. Section 2 reviews related work. Section 3 describes the data and matching process. Sections 4 and present the empirical analysis and results. Section 6 briefly concludes.

Before we begin the analysis, it worthwhile asking why any of this matters. The answer is that overall, nearly every "firm site" in the 2022 CIDB database has a product in at least one of the five NIST functions, but it falls off quickly after that. Just 39% of sites have security products covering two functions, while 21% have security products that cover three of the functions. Just 10% of the sites cover four of the NIST functions, while only 2% of firms have security products covering all five categories. Although the CIDB database may be missing some products, this is quite troubling.

2 Literature

Economic research on cybersecurity investment has developed over the last years. Gordon and Loeb (2002) develop a seminal economic model of information security investment under diminishing marginal returns, demonstrating that optimal cybersecurity spending is bounded and need not approach full protection [5]. While highly influential, the model abstracts away from specific security products and vendors, treating cybersecurity investment as a single financial decision. Anderson (2001) applies microeconomic theory to cybersecurity, emphasizing the role of externalities and misaligned incentives that can lead firms to underinvest relative to the social optimum, particularly when cyber incidents impose costs on others [1].

Prior research examines how firms make cybersecurity decisions in practice. Moore et al. (2016) document widespread adoption of frameworks such as Control Objectives for Information and Related Technology (COBIT). While these frameworks structure security investments and support compliance, they do not explicitly link specific products to reductions in breach likelihood [7]. Consistent with this, Weishäupl et al. (2018) find that cybersecurity investment decisions are frequently driven by compliance obligations, with learning about investment effectiveness occurring in an ad hoc and largely reactive manner [14]. Related evidence suggests that firms may also rely on peer behavior when making security decisions: a study of Finnish information security managers documents herding behavior in cybersecurity investment, with firms following a "let's follow others" strategy when selecting security products [11].

More recent empirical work examines how firm-level security posture affects cyber risk. Gandal et al. (2023) provide robust causal evidence that adopting security products prior to an incident significantly reduces the likelihood of experiencing a data breach [4]. Consistent with this, Kwon and Johnson (2014) show that proactive investments are more effective and more cost-effective, resulting in fewer subsequent breaches and lower notification costs [6].

There is also some empirical evidence on firm decision-making following a breach. Recent research finds that higher breach costs and external detection of incidents lead firms to increase subsequent cybersecurity investment [10]. Bana et al. (2025) show that firms respond to breaches by expanding cybersecurity related human capital, hiring additional IT and security personnel [3]. Similarly, Wang et al. (2025) observe that while firms increase overall IT investment intensity following a breach, they simultaneously experience "threat

rigidity," which leads to a decrease in the initiation of new IT projects [13]. This paper differs from the literature in that we analyze how cyber incidents affect the breadth of security coverage after an attack, as well as how vendor choice changes after an attack. Previous work primarily focused on aggregate investment levels,

3 Data and Descriptive Evidence

3.1 Data

This study uses two main datasets: the Temple Critical Infrasctructure Ransomware Attacks (CIRA) dataset [9], which lists companies that experienced cyber attacks, and the CIDB dataset [12], which tracks IT product installations by firm and vendor in 2018, 2020, and 2022. The CIDB dataset identifies which cybersecurity products are installed in each firm site, as well as the associated vendor. This allows us to construct measures for firms both at the product level and the vendor level over time.[7]

As noted, while we have data from 2018, 2020, and 2022, we do not always know the exact date of the attack, just the year. Hence, it makes sense to use the 2018 data as the "before the attack" period and the 2022 data as the "after attack period." Analyzing data this way compares outcomes sufficiently before and after the 2019-2020 attack window.

A potential complication is that the 2022 CIDB releases employ a different product classification system than the 2018 release. In general, this makes it difficult to compare 2022 deployments directly with 2018. However, since our empirical focus is on differences between attacked and non-attacked firms over time, and since both groups are measured under the same CIDB classification within a given year, this does not pose a problem for our difference-in-difference analysis.

As noted, three of the twenty-four CIDB product series are specific to security: *Security Devices*, *IT Security Information*, and *Network Security Monitoring*. We focus on these series and classify observed deployments into the twelve CIDB security categories. We then map these categories into the five functional categories defined by the National Institute of Standards and Technology (NIST): Identify, Protect, Detect, Respond, and Recover [8]. Table 1 shows the mapping from twelve CIDB categories to the five NIST functions, the number of products in each of the twelve CIDB categories, and the percent of firms adopting products in each the twelve CIDB categories.

[7]To get from the site level to the firm level, we took the products and vendors from each site and aggregated to get the list of unique products and unique vendors at the firm level. If several firm sites used a particular product or vendor, we included it just once.

Table 1: Security Product Categorization and Installation Metrics

CIDB Category	NIST CSF Function	# Products	% Firms
IT Asset Management	Identify	8	3.7%
Advanced Threat Protection	Protect	18	11.6%
Data Loss Prevention	Protect	4	5.0%
Firewall Software	Protect	35	26.9%
Identity Access Management	Protect	63	45.8%
VPN	Protect	17	30.5%
Antivirus	Detect	138	17.6%
Email Security	Detect	7	46.7%
Endpoint Security	Detect	42	22.2%
SIEM	Respond	85	26.6%
Disaster Recovery	Recover	27	11.6%
Other Security	Multiple	33	23.4%

3.2 Outcome Variables

We define four outcome variables in the analysis. The first three measure the breadth of firms' cybersecurity posture.

- First, *NIST Coverage* is the number of NIST functions for which the firm has at least one product deployed, taking values from 0 to 5.
- Second, *CIDB Category Breadth* is the number of distinct CIDB categories (see Table 1) in which the firm has at least one security product. This measure ranges from 0 to 12.
- Third, the *MI CIDB* measures the number of the four Most Important core CIDB categories – Firewall Software, Identity Access Management (IAM), Endpoint Security, and Security Information and Event Management (SIEM) – in which the firms has coverage. This measure ranges from 0 to 4.
- Fourth, the measure *Total Security Products* is the total number of implemented security products employed by the firm. This measure captures the depth of security coverage.

The first three measures are more important than the total number of products, since total products may include duplicate products in a category, i.e., several firewalls.[8]

3.3 Matching Process

The CIRA dataset identifies 102 US firms that publicly disclosed ransomware attacks in 2019 and 2020 (36 in 2019 and 68 in 2020). To construct a comparison group, we match each attacked firm to a non-attacked firm in the 2018 CIDB dataset by SIC4 industry code

[8]In addition to product-level granularity, the CIDB dataset identifies the vendor supplying each product. This feature allows us to track the number of vendors each firm uses and how vendor portfolios change over time. We discuss this in detail in Section 5.

and firm size (employee count). For each SIC4 code, we select non-attacked firms with the closest employee counts, and manually reviewed the matches. This yields a final dataset of 102 attacked and 102 non-attacked firms.

3.4 Descriptive Statistics

We begin by reporting descriptive statistics regarding the four cybersecurity outcome variables over time. Table 2 reports the mean number of security products for the four outcome variables for both attacked and non-attacked firms in 2018 and 2022.

Table 2 shows that in 2018, prior to the attacks, there was virtually no difference between attacked and non-attacked firms in terms of the four outcome variables which we defined[9].

The Table shows that while all firms expanded cybersecurity NIST products, CIDB security categories, and total security products between 2018 and 2022, attacked firms increased their products in these three areas by more than non-attacked firms. In the case of the four Most Important core CIDB categories (MI CIDB), attacked firms increased their holdings, while non-attacked firms did not!

While the descriptive statistics are informative, in order to determine whether the observed patterns reflect a statistically significant difference between attacked and non-attacked firms, we employ a difference-in-differences empirical (econometric) framework in Section 4.

Table 2: Mean Number of Security Products, NIST functions and CIDB categories and MI CIDB covered for Attacked and Non-Attacked Firms

Year	Group	Total #	NIST	CIDB	MI CIDB
2018	Attacked (N=102)	2.43	1.54	1.87	1.31
2018	Non-Attacked (N=102)	2.46	1.51	2.01	1.41
2022	Attacked (N=102)	6.51	2.42	4.31	1.91
2022	Non-Attacked (N=102)	5.11	1.93	3.59	1.37

4 Empirical Analysis

4.1 Empirical Strategy

We exploit the panel structure of the data, with repeated observations on each firm, to estimate how cybersecurity posture evolves following cyber attacks. Our empirical strategy is a two-period Difference-in-Differences (DID) model design that compares pre-attack and post-attack outcomes for attacked versus non-attacked firms.

We estimate this model on a balanced panel of 204 firms observed in 2018 and 2022. Exactly half of the firms (102) experienced a cyber attack in either 2019 or 2020, while the remaining 102 did not report an attack during this interval. For each firm-year observation,

[9]NIST functions covered, CIDB security categories covered, the four Most Important core CIDB categories (MI CIDB) covered and the total number of security products employed by the firm.

we observe a rich set of security-related variables derived from the CIDB data, including both counts of deployed security products and measures of how broadly these security products (or tools) span the five NIST Cybersecurity Framework functions (Identify, Protect, Detect, Respond, Recover) and the 12 CIDB security categories.

4.2 Econometric Estimation

We define the following variables:

- The variable TREAT equals one if the firm is in the attacked group. We use the notation "TREAT" so that it is consistent with DID models.
- The variable AFTER equals one if we are in the second period, i.e., 2022. Otherwise, AFTER equals zero.

Thus the DID model is as follows:

$$Y_{it} = \beta_0 + \beta_1 \cdot \text{TREAT}_{it} + \beta_2 \cdot \text{AFTER}_{it} + \beta_3 \cdot \text{TREAT}_{it} \cdot \text{AFTER}_{it} + \varepsilon_{it}, \tag{1}$$

where Y_{it} denotes the cybersecurity "outcome" for firm i in year t and The error term ε_{it} captures idiosyncratic shocks. This is a Difference-in-Differences model. To see this, we can take expectations (EXP):

- EXP $[Y_{it}|TREAT = 0, AFTER = 0] = \beta_0$
- EXP $[Y_{it}|TREAT = 1, AFTER = 0] = \beta_0 + \beta_1$
- EXP $[Y_{it}|TREAT = 0, AFTER = 1] = \beta_0 + \beta_2$
- EXP $[Y_{it}|TREAT = 1, AFTER = 1] = \beta_0 + \beta_1 + \beta_2 + \beta_3$

We can calculate the differences between the "before" and "after" period for each of the two groups of firms [attacked and non-attacked]:

- The difference for the treated (attacked) group between the before and after periods is $[\beta_0 + \beta_1 + \beta_2 + \beta_3] - [\beta_0 + \beta_1] = \beta_2 + \beta_3$
- The difference for the non-treated (non-attacked) group between the before and after periods is $[\beta_0 + \beta_2] - [\beta_0] = \beta_2$
- Thus the "difference in the difference" between the two groups is $[\beta_2 + \beta_3] - [\beta_2] = \beta_3$[10]
- Hence, the effect of the treatment, i.e., the difference between attacked and non-attacked firms in the post attack period is measured by β_3. This is the primary parameter of interest.
- The interpretation of the other two parameters are as follows: The difference between the attacked and non attacked group in the "pre attack" period is measured by β_1. The time effect is measured by β_2.

[10] This is why the model is called a Difference-in-Differences (DID) model.

Table 3: DID Regressions Main Results — 2018 vs 2022

	(1) NIST Functions	(2) MI CIDB Categories	(3) Overall CIDB Categories	(4) Total # of Security Products
DiD model				
AFTER (β_2)	0.412***	−0.039	1.578***	2.618***
	(0.122)	(0.122)	(0.297)	(0.588)
TREAT (β_1)	0.020	−0.098	−0.137	−0.108
	(0.130)	(0.129)	(0.253)	(0.328)
AFTER*TREAT (β_3)	0.471***	0.637***	0.863**	1.510
	(0.171)	(0.185)	(0.409)	(0.929)
R-squared	0.081	0.035	0.113	0.092
Observations	408	408	408	408

Notes: The Table reports estimates from the Difference-in-Differences (DID) specification. Clustered Standard errors at firm level in parentheses. The model compares attacked and non-attacked firms between 2018 and 2022.
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

4.3 Results

Table 3 presents DID regression estimates comparing firm-level cybersecurity posture between 2018 and 2022. The Table shows that generally there is growth in cybersecurity adoption over this period, as shown by the estimate of the common time effect (β_2), even among firms that did not experience a cyber attack. The estimates of this parameter are beside the variable "AFTER" in the Table. Thus, both attacked and non-attacked firms expanded the total number of deployed products, increased coverage across NIST functions, and adopted a broader set of the CIDB security product categories, reflecting general trends in cybersecurity investment.

As we noted, the main parameter of interest in Table 3 is β_3, the difference in difference effect of being attacked vs. not being attacked. The estimates of this parameter are the ones beside the variable "AFTER*TREAT" in the Table.[11] Controlling for the common time effect (β_2), the change made by attacked firms in the key three security measures following a cyber attack is much greater than the change for firms that were not attacked. Relative to 2018 (pre-attack), by 2022 (post-attack) firms that suffered cyber incidents increased NIST functionality, added more of the twelve CIDB categories and more "MI CIDB" technologies than non-attacked firms. All three of the these estimates of β_3 are statistically significant. In the case of total products, the effect is not statistically significant. But as noted, the other three measures are much more important than the total number of products, since total products may include duplicate products in a particular CIDB category, e.g., several firewalls.[12]

Note that the estimate of β_1 is not statistically significant. The estimates of this parameter are the ones beside the variable "TREAT" in the Table. It measures the pre-attack difference between the attacked and non-attacked groups. This means that there was no

[11]The results are qualitatively unchanged if we run separate regressions for those attacked in 2019 and 2020.

[12]Subgroup analysis for firms attacked in 2019 and 2020 shows broadly the same patterns.

statistically significant difference between the attacked and non-attacked firms before the attacks regarding the four outcome variables.

4.4 Fixed Effect (FE) Model Estimation

Instead of the DID model, another way to estimate the model is via fixed effects. We will not describe that model in detail. Since we have two periods, the estimate of the parameters are identical for both models. In particular, the estimate of β_3, in the fixed effects model, is exactly the same as in the DID model. Similarly, the estimate of the time effect parameter β_2 is also exactly the same.[13] The DiD model explicitly includes the variable TREAT, which means that we can estimate the average baseline difference in security posture between attacked and non-attacked firms in the DID model, that is, the parameter β_1. The fixed effects model cannot estimate that parameter.[14] The DID model is a bit simpler and easier to understand.

5 Security Vendor Changes

Beyond changes in overall security posture, cyber attacks may also alter the composition of firms' "security vendor" portfolios. By security vendors, we mean those vendors that sell security products as defined by the CIDB. Hence, we know the vendors for the 507 security products in the CIDB.

Vendor choice is an economically meaningful margin because switching across vendors entails adjustment costs (e.g., integration, compatibility, and training). To capture vendor-level adjustments, we classify vendors along two dimensions. First, the "Largest 5 vendors" are defined as the five vendors with the largest market share in a given year, where market share is measured as the share of sites in a category that use a given vendor. Second, "platform vendors" are defined as those who supply products in at least two distinct security categories, reflecting broader product scope.

Table 4 presents the corresponding classification for 2020 across the four most important CIDB categories. The Table shows that no vendor appears in the Table twice. In the conclusion we will discuss the importance of this.

Table 5 reports the mean number of Largest 5 and Platform security vendors for attacked and non attacked firms in 2018 and 2022. The Table shows that non-attacked and attacked firms differed somewhat in vendor portfolios before the attack. In particular, before the attacks, non-attacked firms used 36 percent more "largest 5 vendor" products than attacked firms and 38 percent more "platform vendor" products than attacked firms.

The change between 2018 and 2022 for attacked firms was dramatic: the mean number of security products for attacked firms from the largest 5 vendors increased by 100 percent, while the mean number of security products for attacked firms from platform vendors increased by 141 percent. The percent change in these categories for non-attacked firms was more more

[13] The standard errors are identical as well.

[14] Since we do not care that much about the "average baseline difference" between treated and control groups, both models are reasonable in our two-period setting.

Table 4: Largest 5 Vendors by Category (MI CIDB), 2020

Category	Vendor
Endpoint Security	
	Symantec
	Tripwire
	Kaspersky
	Trend Micro
	IBM
Firewall Software	
	Barracuda Networks
	Palo Alto Networks
	Fortinet
	D-LINK
	Cisco Systems Inc
SIEM	
	McAfee Inc.
	Q1 Labs
	Trustwave
	Curalate
	Splunk
Identity Access Management Software	
	RSA Security LLC
	Sailpoint
	Iovation
	IBM
	ThreatMetrix

Table 5: Mean Number of Security Vendors Across Years for Attacked and Non-Attacked Firms

Year	Group	Largest 5 vendors	Platform vendors
2018	Attacked (N=102)	1.84	1.55
2018	Non-Attacked (N=102)	2.51	2.14
2022	Attacked (N=102)	3.68	3.74
2022	Non-Attacked (N=102)	3.79	2.59

moderate. By 2022, attacked firms on average used 44 percent more products from platform vendors than non-attacked firms.

We then we estimated the DID specification in equation (1) using "largest 5 vendors" products and "platform vendor" products as outcomes using 2018 and 2022 data. Because

Table 6: DID Regression Results: 2018 vs 2022

	(1) Largest 5 Vendors	(2) Platform Vendors
DiD model		
AFTER (β_2)	−0.109	2.045***
	(0.225)	(0.292)
TREAT (β_1)	0.029	0.253
	(0.175)	(0.342)
AFTER*TREAT (β_3)	0.754***	1.057***
	(0.287)	(0.406)
R-squared	0.030	0.207
Observations	408	408

Notes: The Table reports estimates from the difference-in-differences (DID) specification. Clustered Standard errors at firm level in parentheses. The model compares attacked and non-attacked firms between 2018 and 2022.
* $p < 0.10$, ** $p < 0.05$, *** $p < 0.01$.

the distribution of the outcome variables is skewed, we use the natural log transformation.[15] Table 6 presents the results. The estimated coefficients of the key parameter (β_3) associated with the variable "AFTER*TREAT" are positive and statistically significant for the largest 5 vendors and platform vendors, indicating that cyber attacks induced firms to reconfigure their portfolios towards vendors with greater market presence and category breadth. Attacked firms significantly shift toward vendors offering broader product coverage and vendors with larger market shares. This pattern suggests that post-incident procurement favors established vendors.

6 Brief Conclusion

Cyber attacks are often thought to change how firms invest in cybersecurity, but there is little empirical evidence on how firms actually adjust after an attack, largely due to the lack of detailed firm-level data. Using unique data that allow us to observe cybersecurity investments at a very delineated level, this paper studies how cyber attacks affect firms' cybersecurity decisions, focusing on the breadth of security products and choice of vendors.

Our analysis evaluated how firms adjusted their cybersecurity posture between 2018 and 2022 along two: (i) breadth of security products, and (ii) reconfiguration of vendor portfolios. Two main findings emerge. First, attacked firms increase the breadth of their security posture relative to non-attacked firms. They adopt more NIST functions and add broader CIDB security category coverage than non-attacked firms. Second, attacked firms

[15]Since there are a small number of "zeros" in the outcome data, we define each outcome as ln(outcome + 0.01).

were more likely to add vendors with large market presence and broader product scope (Largest 5 vendors and platform vendors).

Table 4 shows that in the four most important CIDB categories, no vendor appears in the Table twice. This is encouraging because of the concern about "systemic cyber risk", which we write about in a separate paper [2]. In particular, as we define "**Product-level systemic cyber risk**" as follows in that paper: Product-level systemic cyber risk occurs when there is (i) concentration among technology suppliers and (ii) the products of those suppliers exhibit significant cyber vulnerabilities.

Hence the lack of concentration across the four important CIDB categories is encouraging. Of course, there might be concentration within a category, which would be concerning. It will be important to explore this issue further in future work.

References

[1] R. Anderson. Why information security is hard-an economic perspective. In *Seventeenth annual computer security applications conference*, pages 358–365. IEEE, 2001.

[2] S. Athey, N. Gandal, and T. Moore. Systemic cyber risk: Linking measurement, market incentives, and policy. *SSRN preprint*, 2026. `https://hq.ssrn.com/ffrevision.cfm?abstract_id=5523059`.

[3] S. H. Bana, E. Brynjolfsson, W. Jin, S. Steffen, and X. Wang. Human capital acquisition in response to data breaches. *MIS Quarterly*, 49(1):367–388, 2025.

[4] N. Gandal, T. Moore, M. Riordan, and N. Barnir. Empirically evaluating the effect of security precautions on cyber incidents. *Computers & Security*, 133:103380, 2023.

[5] L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

[6] J. Kwon and M. Johnson. Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, 38(2):451–471, 2014.

[7] T. Moore, S. Dynes, and F. Chang. Identifying how firms manage cybersecurity investment. In *15th Workshop on the Economics of Information Security (WEIS)*, 2016.

[8] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Technical Report NIST CSWP 29, National Institute of Standards and Technology, Gaithersburg, MD, Feb. 2024.

[9] A. Rege. Critical Infrastructure Ransomware Attacks (CIRA) Dataset Version 12.9, 2024. `https://sites.temple.edu/care/cira`.

[10] F. A. Shaikh and M. Siponen. Organizational learning from cybersecurity performance: Effects on cybersecurity investment decisions. *Information Systems Frontiers*, 26(3):1109–1120, 2024.

[11] X. Shao, M. Siponen, and F. Liu. Shall we follow? Impact of reputation concern on information security managers' investment decisions. *Computers & Security*, 97:101961, Oct. 2020.

[12] Spiceworks Ziff Davis. Data Intelligence, 2024. `https://swzd.com/products/data/`.

[13] Q. Wang, C.-H. Peng, Y. Jin, and S. Jiang. Impact of data breach on it investment: Embracing both failure learning and threat rigidity. *Production and Operations Management*, 34(6):1256–1275, 2025.

[14] E. Weishäupl, E. Yasasin, and G. Schryen. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*, 77:807–823, Aug. 2018.