Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains*

Matteo Crosignani
New York Fed

Marco Macchiavelli
UMass Amherst

André F. Silva
Federal Reserve Board

June 2022

Abstract

This paper examines the supply chain effects of the most damaging cyberattack in history so far. The attack propagated from the directly hit firms to their customers, causing a four-fold amplification of the initial drop in profits. These losses were larger for affected customers with fewer alternative suppliers. Internal liquidity buffers and increased borrowing, mainly through bank credit lines, helped firms navigate the shock. Nonetheless, the cyberattack led to persistent adjustments to the supply chain network, with affected customers terminating trading relations with directly hit firms and forming new ones with alternative suppliers with a stronger cybersecurity posture.

JEL Codes: L14, E23, G21, G32.
Keywords: cyberattacks, supply chains, bank credit.

*We thank the editor, Toni Whited, an anonymous referee, Viral Acharya, Tania Babina, Jill Cetina, Miguel Faria-e-Castro, Mariassunta Giannetti, Michael Gofman, Ivan Ivanov, Victoria Ivashina, Huiyu Li, Nicola Limodio, Vojislav Maksimovic, Andreas Milidonis, Camelia Minoiu, Patricia Mosser, Andreas Papaetis, Brian Peretti, Andrea Presbitero, Julien Sauvagnat, Antoinette Schoar, Stacey Schreft, and Jialan Wang for their extremely helpful comments. We are also grateful to the participants at the 2021 NBER Corporate Finance Spring Meeting; London School of Economics; 2020 Federal Reserve System Conference on Financial Institutions, Regulation, and Markets; 2020 OFR/Cleveland Fed Financial Stability Conference; EBRD; Federal Reserve Board; New York Fed; University of Sussex; 2020 Bank of Italy/FRB Conference on Nontraditional Data and Statistical Learning; 2020 EBA Policy Research Workshop; 3rd Endless Summer Conference of Financial Intermediation and Corporate Finance; 2021 SGF Conference; Bank of Italy; ifo Institute, University of Munich; Humboldt University of Berlin; Bentley University; Brattle Group; University of Virginia, Darden; Babson College; UMass Amherst; 2021 Federal Reserve Stress Testing Conference; IV CEMLA Conference on Financial Stability; and 2021 IBEFA Summer Meeting for their suggestions. We also thank Chris Florackis, Christodoulos Louca, Roni Michaely, and Michael Weber for sharing the data on firm-level cybersecurity risk, as well as William Arnesen and Frank Ye for excellent research assistance. The views expressed in this paper are those of the authors and do not necessarily represent those of the Federal Reserve Bank of New York, the Board of Governors of the Federal Reserve System, or other members of their staffs. Emails: matteo.crosignani@ny.frb.org; mmacchiavelli@isenberg.umass.edu; andre.f.silva@frb.gov.

"The world evolves. And the risks change as well. And I would say that the risk that we keep our eyes on the most now is cyber risk. That's really where the risk, I would say, is now, rather than something that looked like the Global Financial Crisis."

—Federal Reserve Chair Jerome Powell, interview on *60 Minutes*, CBS, April 11, 2021

1 Introduction

Cybercrime is now one of the most pressing concerns for firms.[1] Hackers perpetrate frequent cyberattacks mostly for financial gain, while state actors often use more sophisticated techniques to obtain strategic information such as intellectual property and, in more extreme cases, to disrupt the operations of critical organizations. Some severe cyberattacks can spread instantaneously and disrupt the integrity of IT systems, affecting the productive capacity of the directly hit firms and, through supply chain relations, also that of their customers and suppliers. Despite these unique features and their growing importance, there is little evidence on the disruptive effects of cyberattacks on the productive sector. This lack of evidence is largely due to the fact that the existing literature has focused primarily on data breaches, which can affect reputation and litigation risk (e.g., Kamiya, Kang, Kim, Milidonis, and Stulz, 2021) but usually do not affect firms' operations and production of goods and services.

In this paper, we study a particularly severe cyberattack that inadvertently spread beyond its original target and disrupted the operations of several firms around the world. Through supply chain relations, the effects of the cyberattack propagated downstream to the customers of directly hit firms[2]. To cope with the shock, affected customers used their liquidity buffers and increased their reliance on external finance, drawing down their credit lines at banks. We also observe persistent adjustments to the supply chain network in response to the shock, with affected customers more likely to terminate relations with the directly hit firms and create new ones with alternative suppliers with a stronger cybersecurity posture.

[1] For instance, the 2019 World Economic Forum Executive Opinion Survey ranks cyberattacks as the number one risk for CEOs in North America and Europe (WEF, 2019).

[2] We refer to indirectly affected customers of directly hit firms as affected customers throughout the paper.

Specifically, we examine the effect of the most damaging cyberattack in history so far (Greenberg, 2018, 2019). Named NotPetya, the cyberattack was released on June 27, 2017 and targeted Ukrainian organizations in an effort by Russian military intelligence to cripple critical infrastructure in Ukraine. The initial vector of infection was a software that the Ukrainian government required all vendors in the country to use for tax reporting purposes. When this software was hacked and the malware released, it spread across different companies, including large multinational firms through their Ukrainian subsidiaries. For instance, the shipping company Maersk had its entire operations come to a halt, creating chaos at ports around the globe. A FedEx subsidiary was also affected, becoming unable to take and process orders. Manufacturing, research, and sales were halted at the pharmaceutical giant Merck, making it unable to supply vaccines to the US Center for Disease Control and Prevention. Several other large companies (e.g., Mondelez, Reckitt Benckiser, Nuance, and Beiersdorf) had their servers down and could not carry out essential activities.

We provide four main findings. First, we show that the halting of operations among the directly hit firms had a significant negative effect on the productive capacities of their customers around the world, which reported significantly lower profits. A conservative estimate implies a $7.3 billion loss by the affected customers, an amount four times larger than the losses reported by the firms directly hit by the cyberattack. Faced with this temporary shock, affected customers depleted some of their preexisting liquidity buffers and increased the amount of external borrowing, allowing them to maintain investment and employment. While the downstream disruptions to customers were severe, we do not find widespread upstream effects for the suppliers of the directly hit firms.

Second, we investigate the role of supply chain vulnerabilities in driving these effects. We find that the downstream disruption caused by the cyberattack is concentrated among customers that have fewer alternatives for the directly hit supplier. This result holds both when considering how many suppliers a customer has in the same industry as the directly hit supplier and when focusing on suppliers of less substitutable goods and services—i.e., suppliers providing high-specificity goods.

Third, we analyze in detail the role of banks in mitigating the negative liquidity effects of the cyberattack on affected customers. To this end, we use confidential credit register data for the US (the Federal Reserve's Y-14Q corporate schedule), with loan-level information at a quarterly frequency for banks with total assets of more than $50 billion. While there was no change in credit line commitments granted by banks, affected customers drew down their credit lines relatively more

to compensate for the liquidity shortages. In addition, interest rate spreads increased relatively more for affected customers with credit line renewals soon after the shock.

Finally, we examine the dynamic supply chain response to the disruption caused by the cyberattack. We find that the affected customers are more likely to end their trading relations with the suppliers directly hit by the cyberattack, suggesting that the temporary disruptions caused by the cyberattack eroded the reputation of the directly hit firms as reliable suppliers, causing long-lasting effects. We also find that, after the shock, affected customers are more likely to form new trading relations with alternative suppliers (firms in the same industry as the directly hit supplier), particularly those that are less exposed to cybersecurity risk. These findings suggest that the disruption caused by the cyberattack served as a "wake-up call" for the affected customers, which responded by selecting suppliers with a stronger cybersecurity posture, resulting in a more cyber-resilient supply chain.

Our paper contributes to the nascent literature on the economics of cybercrime—an area that is getting increasing attention by both practitioners (Accenture, 2019; Verizon, 2019; Siemens, 2019) and policymakers (US Congress, 2021; Powell, 2021). The academic literature has mostly focused on examining the effects of cyber risk on financial stability (Kashyap and Wetherilt, 2019; Duffie and Younger, 2019; Aldasoro, Gambacorta, Giudici, and Leach, 2022; Eisenbach, Kovner, and Lee, 2021; Kotidis and Schreft, 2022) and developing firm-level measures of exposure to cyber risk using textual analysis (Jamilov, Rey, and Tahoun, 2021; Florakis, Louca, Michaely, and Weber, 2022). Other related papers study abnormal equity returns following data breaches (Kamiya, Kang, Kim, Milidonis, and Stulz, 2021; Garg, 2020; Akey, Lewellen, Liskovich, and Schiller, 2021; Amir, Levi, and Livne, 2018), which, as mentioned before, can lead to reputation and litigation costs but usually do not disrupt firms' operations. In contrast to these studies, we focus on a far more damaging and larger-scale cyberattack resulting in operational disruptions and document its economic and financial effect, through supply chain linkages, on the productive sector at large. These disruptive cyberattacks are becoming more and more frequent, as evidenced by the ransomware attacks on Colonial Pipeline, the largest pipeline system for refined oil products in the United States, and JBS, a global beef processing company. In both cases, operations halted for several days, causing protracted supply chain bottlenecks.

What separates our paper from the existing cyber risk literature is also the emphasis on how the interconnectedness of the digital infrastructure allows a cyberattack to increase its reach and thus

have systemic consequences. In the case we study, Russian military intelligence had to penetrate only one software company to infect all its users through a malicious software update. This type of cyberattack is indeed called a "supply chain attack" since, by compromising one software company and exploiting its connections with a wide range of users, the software users themselves become infected. If the attack is also designed to paralyze the infrastructure of the targets, the shock can become systemic. A related source of interconnectedness responsible for the success and propagation of severe cyberattacks takes place within firms, particularly large multinational corporations. Firms often operate fully integrated IT systems with poor compartmentalization. Thus, by taking over one computer, the hacker can potentially obtain administrative privileges and spread the malware to all the computers of a corporation. This vulnerability ultimately allows the hacker to paralyze the entire operations of a firm for several weeks, as happened in the case of NotPetya. As a result of the lengthy disruption, the shock propagated further down the supply chain to the customers of the directly hit firms. Consequently, we also offer new insights into the theoretical literature on cyber risk. Kamiya, Kang, Kim, Milidonis, and Stulz (2021) provide a theoretical model of firms' optimal exposure to cyber risk. Our results are generally in line with the prediction that the directly hit firms should experience a significant drop in equity prices after the attack. We add to their framework by showing that customers of directly hit firms may face consequences as well and therefore should take into account the cybersecurity of the suppliers when deciding their optimal exposure to cyber risk. We find direct evidence for this mechanism by showing that, after the cyberattack, affected customers form new relations with suppliers that have a stronger cybersecurity posture.

Our paper also complements the literature on supply chain propagation following severe shocks such as natural disasters (Barrot and Sauvagnat, 2016; Boehm, Flaaen, and Pandalai-Nayar, 2019; Carvalho, Nirei, Saito, and Tahbaz-Salehi, 2021) and credit supply shocks (Alfaro, García-Santana, and Moral-Benito, 2021; Cortes, Silva, and Van Doornik, 2019; Costello, 2020). We contribute to this literature by showing that severe but temporary operational disruptions caused by a cyberattack can lead to a permanent reconfiguration of the supply chain network. Specifically, we show that customers of directly hit firms terminate relations with directly hit firms and form new ones with alternative suppliers with stronger cybersecurity—a result particularly relevant for the theoretical literature on endogenous production networks (e.g., Elliott, Golub, and Leduc, 2022).

In addition, cyberattacks are considerably different from natural disasters or credit supply shocks,

with far-reaching consequences in terms of both risk management and identification of the shocks. On the one hand, natural disasters have some seasonal and geographical predictability, thus allowing firms to mitigate their exposure to such risk, and are geographically clustered, making identification of supply chain effects particularly challenging.[3] On the other hand, credit supply shocks tend to be slow moving and often caused by excessive risk-taking, which can be potentially mitigated with micro- and macroprudential policies. Moreover, credit shocks affect firms and households at the same time, causing the estimated effects to be likely driven by both demand and supply forces. Instead, cyberattacks are much more unpredictable, are faster to spread, and usually affect multiple geographical regions at the same time. Some large-scale cyberattacks are also designed with the malign intent to create as much damage as possible and have virtually unlimited reach. Indeed, mitigating cyber risk is extraordinarily challenging. Exploiting the interconnectedness of the digital infrastructure, hackers can penetrate a single software company and design a cyberattack that infects all the software's users around the globe through a malicious update, as in the case we study in this paper.[4]

2 Background on NotPetya

In the intelligence world, few things are what they seem. Petya is the name of a ransomware that circulated in 2016. The victim was infected after opening a PDF file purporting to be the resume of a job applicant and, from there, the ransomware encrypted the master file table that serves as a roadmap for the hard drive, making the data on the computer unreachable. The victim was then asked to make a Bitcoin payment to get the hard drive decrypted. What seemed to be a new version of Petya spread quickly in June 2017. It hit Ukraine the hardest but it also appeared

[3]Firms headquartered outside the area hit by a natural disaster could have significant operations as well as trading relations in the impacted area, as a result blurring the lines between affected and unaffected firms. Some directly affected firms may thus be erroneously classified as customers or suppliers of directly affected firms, potentially overestimating supply chain propagation.

[4]Building a "Zero Trust" architecture to mitigate exposure to cyber risk is very complex and even the most sophisticated organizations remain vulnerable to cyber intrusions. For instance, in 2020 Russian intelligence penetrated the software company SolarWinds and was able to infect its users by releasing a tainted software update. This time, however, the malware was intended for intelligence collection on SolarWinds' users, which include US government agencies and many Fortune 500 companies. Had the SolarWinds attack been weaponized as in the case of NotPetya, it would have likely had devastating consequences.

worldwide. However, this new version was able to spread across networks without needing to obtain administrative access. Even though it appeared to be just another ransomware, as shown in Figure A.1 in the Online Appendix, it was quickly found out that the real intent was not the financial gain from the ransom payment. Indeed, the attack was not even designed to keep track of the decryption codes. Instead, the true intent was to encrypt and paralyze the computer networks of Ukrainian banks, firms, and government. This was not a new version of Petya.

This cyberattack was the handiwork of a hacking group from Russian military intelligence, the GRU. The Russian government had been actively involved in meddling in Ukrainian matters since Ukraine, previously part of the Soviet Union, took steps to build closer ties to NATO. Initially, Russia directed a series of cyberattacks on Ukraine, including its power grid, and then resorted to military action by invading and annexing Crimea. It should also be noted that the timing of the NotPetya attack was, in a way, serendipitous. The ease with which NotPetya spread from network to network without human intervention depended on a never-seen-before piece of code that was leaked in April 2017 by the Shadow Brokers, a hacking group. The leaked code, called EternalBlue, is a very sophisticated tool developed by the US National Security Agency to harvest passwords and move from network to network. EternalBlue was used together with another tool, Mimikatz, that was already circulating among hackers and can find network administrator credentials stored in the infected machine's memory.[5]

NotPetya was itself a supply chain attack, in the sense that the initial point of entry was a backdoor planted in an accounting software, called M.E. Doc, widely used by Ukrainian firms for tax reporting. As a result, most companies operating in Ukraine got infected, including multinational companies through their Ukrainian subsidiaries.[6] More generally, Moody's (2020) argues that companies with less sophisticated cybersecurity are at risk of attacks stemming from suppliers and vendors with access to their IT systems. For instance, a compromised software company can become a vector through which thousands of customers' computers are infected.

[5]Microsoft released a patch for EternalBlue before the NotPetya incident. However, NotPetya could infect unpatched computers, grab the passwords via Mimikatz, and spread to patched computers. Many firms reportedly do not update regularly for fear that the updates could interfere with their software.

[6]More details about NotPetya can be found in Greenberg (2019), a book about NotPetya and other cyberattacks conducted by Russian military intelligence on Ukraine in 2014–2017.

3 Data

We use several data sources to conduct our analysis at both the firm and loan level, including global supply chain relationships data from FactSet Revere, balance sheet data on firms worldwide from Orbis, and credit register data for the US from the Federal Reserve's Y-14Q.

First, to identify the firms directly affected by NotPetya, we start by web scraping filings to the Securities and Exchange Commission in 2017 and 2018.[7] We search for different keywords, including "Petya," "NotPetya," and "cyber." Among the filings that contain a match, we exclude matches that are unrelated, such as cybersecurity firms citing NotPetya as the main cyberattack of the year. We also look for instances in which NotPetya is cited in newspaper articles worldwide. Using the Dow Jones Factiva database, which contains a repository of international newspaper articles, we obtain over 4,500 relevant articles, which we manually check for news about firms directly hit by NotPetya. Finally, we cross-check the list of directly hit firms with Greenberg (2019). We exclude firms in Ukraine and Russia, as well as nonpublic firms that we would not be able to match with other data sets. Overall, as described in detail in Table 1, we identify eight very large publicly-listed firms that were directly hit by NotPetya. We show the geographical and sectoral distribution of these directly hit firms in Figure A.2 and Table A.1 in the Online Appendix, respectively. Half of the directly hit firms are based in the US, with the other companies headquartered in the UK, Germany, and Denmark. In addition, half of the directly hit firms belong to the manufacturing sector, with the other half equally spread between services and transportation. In Figure 1, we show that the stock price of these directly hit firms collapsed by 5% after they disclosed the damages of NotPetya.

Second, we obtain global supply chain relationships data from FactSet Revere, arguably the most comprehensive source of firm-level customer-supplier relationships currently available.[8] Specifically, the data set includes almost one million relationships between large (mostly publicly listed) firms

[7] Starting in 2005, the SEC required publicly traded firms to disclose material factors that may adversely affect their business, operations, or future performance in 10-K filings (providing updates in the subsequent 10-Qs).

[8] Alternative sources of supply chain data either do not have information with sufficiently high frequency on the start and end dates of a relationship between two firms (e.g., Bloomberg, Capital IQ) or are not as granular as FactSet (e.g., Compustat Segment data, which report, with an annual frequency, only the largest customers of a given supplier).

Firm Name	Costs	Additional Details
Beiersdorf *Assets*: $7.69 bln *Industry*: Chemicals and Allied Products (SIC 28) *Country*: Germany	$43 mln	Various locations of the Beiersdorf pharmaceutical group were cut off from mail traffic for days. Beiersdorf said €35 million euros worth of second-quarter sales were delayed to the third quarter, and it was totting up the costs of the attack for items such as calling in outside experts, running promotions, and using other production sites to make up for shortfalls.
FedEx *Assets*: $33.07 bln *Industry*: Transportation by Air (SIC 45) *Country*: US	$400 mln	Delivery service FedEx lost $400 million after NotPetya crippled its European TNT Express business. The reported costs came from loss of revenue at TNT Express and costs to restore technology systems. Six weeks after the attack, customers were still experiencing service and invoicing delays, and TNT was still using manual processes in operations and customer service.
Maersk *Assets*: $68.84 bln *Industry*: Transportation Services (SIC 47) *Country*: Denmark	$300 mln	Maersk reinstalled 4,000 servers, 45,000 PCs, and 2,500 applications over 10 days. The company experienced only a 20% drop in volume, while the remaining 80% of operations were handled manually. Losses of about $300 million included loss of revenue, IT restoration costs, and extraordinary costs. The company was hiring 26 new employees a week, planning to have 4,500 to 5,000 IT employees within 18 months. At Maersk terminals in the Port of New York and New Jersey, computers, phones, and gate systems shut down, forcing the use of paper documents.
Merck *Assets*: $98.17 bln *Industry*: Chemicals and Allied Products (SIC 28) *Country*: US	$670 mln	At Merck, NotPetya temporarily disrupted manufacturing, research and sales operations, leaving the company unable to fulfill orders for certain products, including vaccines. The attack cost Merck about $670 million in 2017, including sales losses and manufacturing and remediation-related expenses.
Mondelez *Assets*: $66.82 bln *Industry*: Food and Kindred Products (SIC 20) *Country*: US	$180 mln	The global logistics chain of the food company Mondelez was disrupted by NotPetya. The forensic analysis and restoration of all IT networks cost $84 million. Added to this expense was the loss of sales. Altogether, Mondelez had to record $180 million of damage by the attack.
Nuance *Assets*: $5.82 bln *Industry*: Business Services (SIC 73) *Country*: US	$92 mln	NotPetya affected Nuance's cloud-based dictation and transcription services for hospitals. Nuance estimated a negative effect of $68 million in lost revenues and $24 million in restoration costs.
Reckitt Benckiser *Assets*: $24.19 bln *Industry*: Chemicals and Allied Products (SIC 28) *Country*: UK	$117 mln	Reckitt Benckiser was hit by NotPetya, halting production, shipping and invoicing at a number of sites. The British consumer goods company suffered $117 million in losses, 1% of annual sales.
WPP *Assets*: $41.55 bln *Industry*: Business Services (SIC 73) *Country*: UK	$15 mln	UK multinational advertising firm WPP was hit by NotPetya, costing about $15 million before insurance. The damage was limited by the fact that WPP's systems are not fully integrated.

Table 1: Firms Directly Affected by NotPetya. This table reports the firms directly affected by NotPetya and their total assets, reported costs associated with the cyberattack, and additional details. Source: SEC Filings; Dow Jones Factiva.

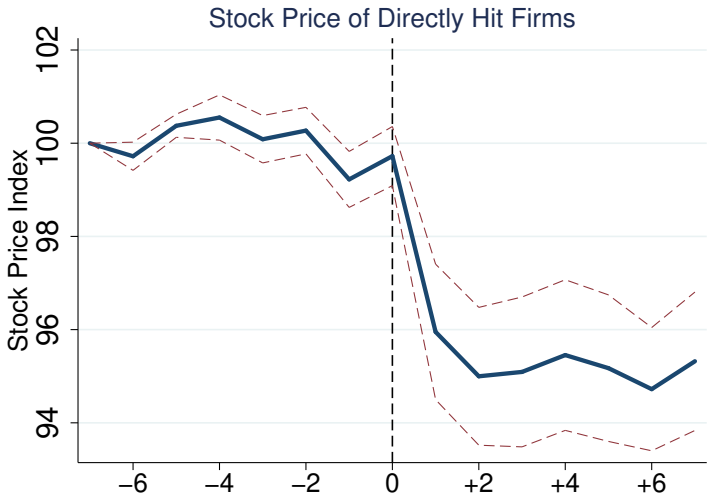

Figure 1: Stock Price of Directly Hit Firms around News of the Damages of NotPetya. This figure shows the stock price evolution around the news of the damages of NotPetya (from seven trading days before the news to seven days after the news). Stock prices are averaged across firms and normalized to 100 seven trading days before the disclosure of the news. The dashed lines indicate the standard deviation around the mean. The dates when the news of the damages were publicly released are as follows: August 16, 2017 for Maersk (link); August 2, 2017 for Beiersdorf (link); June 28, 2017 for Mondelez (link); August 22, 2017 for WPP (link); June 28, 2017 for Nuance (link); July 16, 2017 for FedEx (link); July 5, 2017 for Reckitt Benckiser (link); October 26, 2017 for Merck (link). Source: Thomson Reuters Datastream.

around the world. Each customer-supplier relationship has information on the start date, end date, and relationship type. FactSet collects this information through the firms' public filings, investor presentations, websites, corporate actions, press releases, and news reports. Following Gofman, Segal, and Wu (2020), we drop redundant relationships whose start and end dates fall within the period of a longer relationship between the same firm pair and combine multiple relationships between two firms into a continuous relationship if the time gap between two relationships is shorter than six months. Using each firm's International Securities Identification Number (ISIN), we are able to identify a total of 233 customers and 320 suppliers indirectly affected by the cyberattack—i.e., exposed through their supply chain connections to directly hit firms. As illustrated in Figure A.3 and Figure A.4 in the Online Appendix, customers and suppliers of directly hit firms are spread throughout the world but are particularly prevalent in the US. Around half of these firms in the supply chain belong to the manufacturing sector, while the rest belong to the services, trade, mining, construction, and agriculture, forestry, and fishing sectors (Table A.1).

Third, we collect balance sheet and income statement information on firms worldwide from Orbis—a database by Bureau Van Dijk (part of Moody's Analytics) that contains data for more

than 350 million companies globally. In addition to its extensive coverage, Orbis is particularly attractive due to its cross-country comparability since the data provider organizes the information in a standard global format (Kalemli-Ozcan, Sørensen, Villegas-Sanchez, Volosovych, and Yesiltas, 2022). We merge Orbis with FactSet using the ISIN of each firm and disregard companies that are not present in both data sets to avoid selection bias due to the inclusion of smaller listed firms that appear in Orbis but that do not report supply chain relations. In addition, as is standard in the literature, we remove financial firms and firms in the government sector. We obtain an intersection of 70,590 firm-year observations, corresponding to 15,781 firms from 2014 to 2018, the most recent date available in Orbis.

Finally, we obtain loan-level information on bank credit to firms from the corporate loan schedule (H.1) of the Federal Reserve's Y-14Q. These data have been collected since 2012 to support the Dodd-Frank Act's stress tests and assess bank capital adequacy for large banks in the US. The credit register provides confidential information at a quarterly frequency on credit exposures exceeding $1 million for banks with more than $50 billion in assets. These loans account for around 75 percent of all commercial and industrial lending volume during our sample period. In addition to the amount of committed credit between each firm-bank pair, the data set also contains information on the committed and drawn amounts on credit lines, the amount that is past due, and information on other loan characteristics, such as the interest rate spread, maturity, and collateral. To identify firms indirectly affected by the cyberattack, we merge the firm-bank data for the US with Orbis and FactSet using firms' tax identifiers and CUSIPs, resulting in a sample of 166,895 bank-firm-quarter observations from 2014:Q1 to 2018:Q4, corresponding to 37 banks and 2,133 firms.

4 Identification Strategy

4.1 Firm-Level Analysis

Our objective is to document the effects of the NotPetya cyberattack through the supply chain. Given that the attack caused the directly hit firms to halt operations for several weeks, we are interested in estimating the effects on these firms' customers and suppliers. We use a difference-in-differences approach, comparing the change in behavior of firms indirectly affected by the shock through their

supply chain with that of unaffected firms operating in the same industry, country, and size quartile in the same year. Specifically, we estimate the following model:

$$Y_{ijt} = \alpha + \beta \text{Post}_t \times \text{Affected}_i + \xi_i + \eta_{jt} + \epsilon_{ijt} \tag{1}$$

where i corresponds to a firm, t to a year between 2014 to 2018, and j to the peer group of firm i—an industry-country-size quartile combination in the baseline case, with industries defined at the SIC2 level. Y_{ijt} is one of several outcome variables we consider, including the ratio of earnings before interest and taxes (EBIT) to total assets, the ratio of long-term debt to total assets, and the liquidity ratio (current assets minus inventories over current liabilities). $Affected_i$ is a firm-level indicator variable equal to one if a firm is connected (as a supplier or as a customer) to a directly hit firm. *Post* equals one for 2017 and 2018, the two periods after the June 2017 cyberattack. We estimate the β coefficient within a peer group, captured by the fixed effects η_{jt}.

In robustness tests, we consider alternative peer groups of firms that, in the current year, are in the same industry (or country) and size quartile as the treated firm and, in addition, have a supply chain link with a firm in the same industry as a directly hit firm. This requirement ensures that firms in the control group are not only in the same industry/country and size quartile as the treated firm, but also that they use comparable suppliers. We also include firm fixed effects ξ_i. Standard errors are double clustered at the industry and country level.

The NotPetya cyberattack hit many firms in Ukraine, including the Ukrainian subsidiaries of international firms, and then spread to the entire network infrastructure of most of these companies, affecting their global operations. Importantly for our identification strategy, the attack came from a third-party vendor whose software is widely used in Ukraine for tax filing purposes. Hence, within the set of international firms, it is plausible to assume that the attack was unrelated to firm characteristics. Nevertheless, one may still argue that the severity with which each firm was hit depends on the adoption of best practices to improve cybersecurity, or "cyber hygiene." However, we go one step further and study the effect on customers and suppliers of the directly hit firms. As a result, even if the severity of the attack on the directly hit firms may depend on their cybersecurity practices, it is unlikely that the attack was correlated with characteristics of the indirectly affected firms—either customers or suppliers. In addition, as we show later, affected customers and similar

		Full	Size Q1		Size Q2		Size Q3		Size Q4	
	Stat	Sample	Treated	Control	Treated	Control	Treated	Control	Treated	Control
No. Obs.	Tot	70590	267	51938	268	13778	267	3075	271	726
Age	μ	32.84	28.66	31.01	36.87	36.53	50.09	42.22	53.19	40.37
	p(50)	24.00	22.00	23.00	28.00	25.00	31.00	30.00	34.00	29.00
	σ	26.95	22.36	24.53	27.97	31.10	46.03	34.06	44.23	33.33
Assets (M)	μ	3718	622	446	5537	4409	26366	21616	135840	91691
	p(50)	498	444	284	5149	3483	24651	18850	116539	71886
	σ	15673	526	450	3103	2643	10580	9237	90353	60991
EBIT/Assets	μ	0.04	0.00	0.03	0.06	0.07	0.07	0.06	0.06	0.06
	p(50)	0.05	0.07	0.05	0.06	0.06	0.07	0.05	0.06	0.05
	σ	0.17	0.25	0.19	0.11	0.07	0.07	0.06	0.06	0.06
Liquidity Ratio	μ	1.95	3.04	2.17	1.62	1.35	1.11	1.13	1.26	1.02
	p(50)	1.24	1.58	1.36	1.15	1.07	0.88	0.94	0.91	0.9
	σ	3.02	5.76	3.38	1.84	1.31	0.83	1.17	1.49	0.70
LT Debt/Assets	μ	12.95	8.75	9.88	21.87	20.76	21.96	25.01	21.96	24.35
	p(50)	7.64	2.13	4.10	19.96	18.47	21.64	23.43	21.07	23.21
	σ	15.05	13.41	13.37	16.96	16.38	13.25	15.43	11.90	12.85
ROA	μ	1.78	-1.04	1.06	3.44	3.89	4.71	3.61	4.63	3.68
	p(50)	3.35	5.15	3.28	4.12	3.60	4.48	3.03	4.34	2.96
	σ	12.99	22.19	14.50	7.80	6.68	6.62	5.56	5.47	5.09
No. Employees	μ	9679	2969	2436	22921	15007	63428	47980	127159	100355
	p(50)	1968	1557	1050	9905	8182	40655	27810	95245	66000
	σ	31110	3491	5134	41897	32294	63853	65621	102907	98518
Cost of Employees/Assets	μ	0.14	0.14	0.16	0.09	0.10	0.11	0.08	0.09	0.05
	p(50)	0.09	0.10	0.10	0.06	0.05	0.10	0.04	0.06	0.04
	σ	0.20	0.12	0.21	0.09	0.19	0.08	0.13	0.07	0.05
Tang. Fixed Assets/Assets	μ	0.28	0.22	0.26	0.25	0.33	0.27	0.38	0.24	0.39
	p(50)	0.23	0.18	0.22	0.16	0.28	0.21	0.34	0.20	0.36
	σ	0.23	0.18	0.22	0.21	0.24	0.22	0.26	0.19	0.26

Table 2: Summary Statistics. This table shows summary statistics for our sample firms. The table reports mean, median, and standard deviation. The sample period is 2014 to 2018. The table shows the summary statistics for the full sample as well as the summary statistics for treated and control firms in each of the four size bucket groups. Treated firms are customers of a directly affected firm. Age is in years. Assets are in millions of USD. The liquidity ratio is 100*(current assets – inventories)/current liabilities. Long-term debt (LT Debt) is financial debt with a maturity greater than one year. All the variables divided by total assets (A) are expressed as ratios. However, for ease of interpretation of the estimates, LT Debt/A is multiplied by 100. Source: BvD Orbis; FactSet Revere.

but unaffected firms share similar trends across different outcomes before the cyberattack.

Consider a stylized example of two US firms (A and B) of similar size, both producing medical equipment. Firm A uses Maersk for shipping, while firm B uses Evergreen Marine. By virtue of having a subsidiary in Ukraine, Maersk is hit by NotPetya, while Evergreen Marine has a subsidiary in Greece and, as a result, is not hit by the cyberattack. Therefore, firm A is classified as an affected customer, while firm B is in the control group. The difference-in-differences coefficient β estimates the differential response of firm A relative to firm B after the occurrence of the cyberattack.[9]

The summary statistics of Table 2 show that firm characteristics are similar across affected customers (treatment group) and unaffected firms (control group) within size quartiles—which are constructed relative to the sample of affected firms so as to select firms in the control group that are similar in size to the treated firms.[10] Across size quartiles, firms in the treatment and control groups have similar profitability (EBIT-to-assets ratio), liquidity ratio (current assets net of inventories divided by current liabilities), and reliance on long-term debt (ratio of long-term debt to total assets). Slight differences between treated and control firms are accounted for in the empirical analysis by using industry-country-size-year fixed effects, which allow us to compare a treated firm with a set of control firms within the same industry, country, and size group. In addition, we show that treated and control customers share similar trends in the outcome variables before the cyberattack, addressing residual concerns that pre-existing differences across groups before the shock may drive our results.

4.2 Loan-Level Analysis

While the firm-level analysis allows us to examine the effect of the cyberattack on the affected customers and suppliers' balance sheets, we also use firm-bank matched loan-level data for the US

[9]There is a possibility that some private firms got hit by NotPetya but did not report it. Indeed, the SEC requires only publicly traded firms to do so. The customers of directly hit private firms could therefore be entering the control group when, instead, they should be classified as treated. While we cannot rule out such a possibility, it is important to note that this scenario would generate an attenuation bias—that is, our estimates can be considered a lower bound.

[10]Given that we do not find economically and statistically significant effects for affected suppliers, we show the summary statistics on suppliers in Table A.2 in the Online Appendix. Table A.3 in the Online Appendix is a version of Table 2 where the sample period is restricted to the pre-period (2014–16).

to test the effect of the shock on the amount and terms of bank credit. The specification we use is as follows:

$$Y_{ibjt} = \alpha + \beta \text{Post}_t \times \text{Affected}_i + \xi_i + \eta_{jt} + \gamma_{bt} + \epsilon_{ibjt} \tag{2}$$

where i corresponds to a firm, b to a bank, t to a quarter between 2014:Q1 and 2018:Q4, and j to the peer group of firm i—an industry-state-size quartile combination in the baseline case, with industries defined at the SIC2 level. As before, $Affected_i$ is a firm-level indicator variable equal to one if a firm is connected (as a supplier or as a customer) to a directly hit firm, and $Post$ is a dummy variable equal to one after the June 2017 cyberattack. All specifications control for time-varying bank characteristics using bank-quarter fixed effects γ_{bt}, which absorb bank-specific shocks to credit supply.

The outcome variable Y_{ibjt} is either the logarithm of total committed credit, the logarithm of total committed credit lines, the share of the committed line of credit that is drawn down, the interest rate spread, the bank's subjective default probability of the borrower, a dummy equal to one if the loan is nonperforming, the maturity of the committed exposure, or the logarithm of one plus the amount of collateral. Standard errors are double clustered at the industry and bank level.

5 Results

This section presents our results. In Section 5.1, we show that the cyberattack had a significant negative effect on the profits of customers of the directly hit firms. In Section 5.2, we highlight that the downstream effects are driven by customers with fewer alternatives to the directly hit supplier. In Section 5.3, we report that, in response to the supply chain disruptions caused by the cyberattack, affected customers depleted their preexisting liquidity buffers and increased borrowing. In Section 5.4, we use loan-level data for the US to show that affected customers drew down their credit lines and were charged higher interest rates after the shock. In Section 5.5, we document that the cyberattack also led to persistent adjustments to the supply chain network, with affected customers more likely to terminate relations with the directly hit firms and create new ones with alternative suppliers.

5.1 Propagation of the Cyberattack

Table 3 reports the coefficient estimates of Equation (1) separately for affected customers (Panel A) and affected suppliers (Panel B). In Panel A (B), the control group consists of similar firms to the affected customers (suppliers), but that did not have trading relations with the firms directly hit by the cyberattack. The dependent variable is the ratio of EBIT to total assets. In column (1), we include firm and industry-country-year fixed effects, while in column (2) we use firm and industry-size quartile-year fixed effects. Column (3) reports the results using our preferred specification with industry-country-size-year fixed effects, where the control group consists of firms in the same combination of country, industry, and size quartile as the treated firms. As a robustness test, in columns (4) and (5), the control group consists of firms not only in the same industry (or country) and size quartile as the treated firm, but also with suppliers (Panel A) or customers (Panel B) in the same industry as the directly hit firms. Following our previous example, if medical equipment producer A is treated by virtue of using Maersk (directly hit by the cyberattack) for shipping services, the control group in column (5) would include medical equipment producer B of similar size as firm A, but reporting a shipping company that was not hit by the cyberattack as a supplier.

The results reported in Panel A show that the disruption caused by the cyberattack was strongly propagated downstream, leading to a significant drop in customers' profitability relative to similar but unaffected firms. Specifically, the coefficient estimate in column (3) indicates that the shock led to a 1.3 percentage point drop in EBIT to assets, corresponding to 25 percent of the sample median. The magnitude of the effect is in line with the fact that the cyberattack was severe and caused operations to halt at the directly hit firms for about three to four weeks in many cases.[11] The coefficient of interest is stable across the different types of specifications. For instance, the coefficient in column (3), where we compare affected with unaffected firms in the same industry, country, size quartile, and year, is virtually identical to that in column (5), where we compare affected with unaffected firms in the same industry, size quartile, and year, and with suppliers in an affected industry.

[11] Since profits equal revenues minus both variable and fixed costs (which need to be paid regardless of the output produced), it is expected that the decline in profits is more than proportional to the fraction of the year for which the directly hit firms were not operational.

It is important to note that the downstream supply chain effects of the cyberattack are sizable. The damages to the directly hit firms in our sample add up to $1.8 billion (see Table 1), while a conservative estimate of the supply chain effects on customers suggests a drop in profits by $7.3 billion—a four-fold amplification of the initial drop in profits.[12]

In Panel A of Table A.4 of the Online Appendix, we show that the documented downstream effect is robust to an alternative definition of the treatment variable, where $\widetilde{\text{Affected}}_i$ is a continuous variable equal to the reported costs suffered by the directly hit firm with which each customer had a relationship at the time of the cyberattack (shown in Table 1), normalized by its total assets, and zero for unaffected firms in the control group. In addition, in Panel B of Table A.4, we show that the main results are robust to clustering the standard errors at the industry-upstream industry level. We do not find further downstream propagation of the shock beyond the affected customers. Indeed, in Table A.5 of the Online Appendix, we show that there is no effect on profitability among the customers of the affected customers.[13]

Turning to the estimation of the upstream effect of the attack (Panel B of Table 3), we find a negative but statistically insignificant effect of the shock on the profitability of affected suppliers. This asymmetry, with strong downstream but limited upstream effects, is well established in the existing theoretical and empirical supply chain propagation literature. Specifically, Acemoglu, Akcigit, and Kerr (2016), show both theoretically and empirically that supply-side productivity shocks propagate downstream more strongly than upstream. In fact, when production technologies and consumer preferences are Cobb-Douglas, as is standard in the literature, there is no upstream propagation following supply-side shocks, such as the one we study, since the quantity and price effects cancel each other out.[14] Instead, downstream propagation to customers occurs because an adverse productivity

[12] This estimate is obtained by combining the coefficient of column (3) in Table 3 with summary statistics on the number of firms, EBIT over assets, and average assets for each size quartile from Table 2.

[13] In Table A.5, where we estimate the effect of the cyberattack on the customers of affected customers, we use only the baseline fixed effects, the most saturated being the industry-country-size-year ones in column (3). We do not use the alternative fixed effects that rely on the "Linked to Affected Industry" indicator variable since those are only meaningful in the context of estimating the effect of the cyberattack on the affected customers of the directly hit firms.

[14] Any effect on upstream suppliers depends on the balance between a quantity effect (directly hit firms produce less, reducing their demand for inputs from suppliers) and a price effect (each output produced by the directly hit firms becomes more expensive, raising their demand for inputs from suppliers). With Cobb-Douglas technologies and preferences, these two effects cancel each other out.

Panel A: Customers	(1)	(2)	(3)	(4)	(5)
	EBIT/Assets				
$Post_t \times Affected_i$	-0.010**	-0.012**	-0.013**	-0.015**	-0.012**
	(0.004)	(0.006)	(0.006)	(0.006)	(0.006)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748

Panel B: Suppliers					
	EBIT/Assets				
$Post_t \times Affected_i$	-0.003	-0.003	-0.005	-0.000	-0.002
	(0.005)	(0.004)	(0.004)	(0.003)	(0.004)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	60,019	45,316	45,568
R-squared	0.757	0.740	0.776	0.748	0.747

Table 3: Effect on Profitability, Customers and Suppliers. This table presents results from Equation (1). The sample period is 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. In Panel A, $Affected_i$ is a dummy equal to one if firm i is a customer of a directly hit firm. In Panel B, $Affected_i$ is a dummy equal to one if firm i is a supplier of a directly hit firm. The indicator variable "Linked to Affected Industry" equals one for firms that have supply chain links to industries where directly hit firms operate. The dependent variable is EBIT divided by assets. Standard errors are double clustered at the industry and country level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

shock leads to an increase in the price of the directly hit firms' output. This effect implies a higher production cost for the directly hit firms' customers, reducing their demand for the good produced by the directly hit firm and decreasing the customers' total output.[15] In line with the standard general equilibrium models with input-output linkages, Alfaro, García-Santana, and Moral-Benito (2021)

[15]Instead, theory predicts that demand shocks (e.g., from imports or government spending) should propagate upstream more strongly than downstream (Acemoglu, Akcigit, and Kerr, 2016). Consistent with this prediction, Ozdagli and Weber (2021) show that expansionary monetary policy shocks, by acting as final demand shocks, propagate upstream through the production network. In a different stream of work, Welburn and Strong (2021) build a quantitative model to assess the upstream and downstream propagation of cyberattacks through production networks.

show empirically that credit supply shocks propagate more strongly downstream than upstream, and that industries that are hit harder by such shocks display larger increases in output prices. Similarly, Demir, Javorcik, Michalski, and Ors (2022) show that an unexpected shock that increased the cost of import financing in Turkey got transmitted downstream but not upstream.

5.2 Disruptions and Supply Chain Vulnerabilities

What supply chain features make customers more vulnerable to the disruptions caused by the cyberattack? As firms need several intermediate inputs and services in their production function, they become more vulnerable to sudden interruptions if they cannot easily substitute the supplier that is hit by a shock (e.g., Elliott, Golub, and Leduc, 2022). Hence, we hypothesize that affected customers that have fewer suppliers in the same industry as the directly hit supplier may face more production difficulties and therefore display a larger decline in profitability. Similarly, we also test whether the customers of directly hit suppliers that produce highly specific goods were hit relatively more in terms of profitability. To do so, we split our main coefficient of interest, $\text{Post}_t \times \text{Affected}_i$, into two depending on whether affected customers have more or less than five suppliers (the sample median) in the same industry as the directly hit firm. Specifically, we estimate the following model:

$$\begin{aligned} Y_{ijt} = \alpha + \beta_1 \text{Post}_t \times \text{Affected}_i \times \mathbb{1}(\text{Suppliers} < 5)_i + \\ \beta_2 \text{Post}_t \times \text{Affected}_i \times \mathbb{1}(\text{Suppliers} \geq 5)_i + \xi_i + \eta_{jt} + \epsilon_{ijt} \end{aligned} \tag{3}$$

where, in addition to the variables defined in Equation (1), $\mathbb{1}(\text{Suppliers} < 5)_i$ is an indicator variable equal to one if, at the time of the shock, firm i has less than five suppliers in the directly affected industry to which it is connected. Conversely, $\mathbb{1}(\text{Suppliers} \geq 5)_i$ equals one if firm i has five or more alternative suppliers.

The results of Equation (3) are reported in Table 4 and show that the effect of the supply chain disruption is concentrated among customers with few alternative suppliers. For instance, affected customers with less than five suppliers see a reduction in profits by 3 percentage points relative to the control group, while affected customers with five or more suppliers do not experience any significant change in profits (column 3). The results are similar in columns (4) and (5), which employ alternative fixed effects that require control firms to also be linked to affected industries. Consistent

	(1)	(2)	(3)	(4)	(5)
	EBIT/Assets				
$\text{Post}_t \times \text{Affected}_i \times \mathbb{1}(\text{Suppliers}<5)_i$	-0.024**	-0.025**	-0.030**	-0.026**	-0.026**
	(0.009)	(0.012)	(0.013)	(0.011)	(0.013)
$\text{Post}_t \times \text{Affected}_i \times \mathbb{1}(\text{Suppliers}\geq 5)_i$	0.001	0.002	0.003	-0.004	0.002
	(0.006)	(0.005)	(0.009)	(0.007)	(0.005)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748

Table 4: Effect on Customers' Profitability, Heterogeneity across Number of Suppliers. This table presents results from Equation (3). The sample period is 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable is EBIT divided by assets. The indicator variable $\mathbb{1}(\text{Suppliers} < 5)_i$ is equal to one if, at the time of the shock (July 2017), firm i has less than five suppliers in the affected industry. The indicator variable $\mathbb{1}(\text{Suppliers} \geq 5)_i$ is equal to one if, at the time of the shock (July 2017), firm i has five or more suppliers in the affected industry. The indicator variable "Linked to Affected Industry" equals one for firms that have supply chain links to industries where directly hit firms operate. Standard errors are double clustered at the industry and country level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

with the endogenous network model of Elliott, Golub, and Leduc (2022), these findings suggest that firms with more vulnerable supply chains are hit harder when one of their suppliers is temporarily shut down.

It is important to note that Equation (3) is not a triple difference estimator since the indicator variable $\mathbb{1}(\text{Suppliers} < 5)_i$ is well defined only for the treatment group. Indeed, by construction, firms in the control group have no trading relations with any directly hit firm and thus have no firms from which to substitute away. Nonetheless, in Table A.6 of the Online Appendix we flexibly define $\mathbb{1}(\text{Suppliers} < 5)_i$ for the control group using the average number of suppliers in any affected industry and estimate a triple difference model. The results are qualitatively unchanged to those obtained when estimating Equation (3) and splitting the coefficient of interest into two.

In Table A.7 of the Online Appendix, we use output specificity as a different measure of supply chain vulnerability. An affected customer is considered more vulnerable if the directly hit supplier

produces highly specific outputs.[16] In line with Barrot and Sauvagnat (2016) and Boehm, Flaaen, and Pandalai-Nayar (2019), the results of Table A.7 show that disruptions are more severe when the directly hit supplier produces a more specific and therefore less substitutable product. Indeed, the disruption for affected customers that purchase highly specific products from the directly hit suppliers is statistically significant, while it is, for the most part, insignificant and of smaller magnitude when the directly hit firm produces non-specific goods.

Although the upstream propagation of the cyberattack on the average affected supplier is statistically insignificant (Panel B of Table 3), we also test whether suppliers with more vulnerable supply chains are affected by the shock. Specifically, in Table A.8 of the Online Appendix, we split the main coefficient of interest ($\text{Post}_t \times \text{Affected}_i$) into two, depending on whether affected suppliers have more or less than five alternative customers. In Panel A, we find that the upstream effect is negative, albeit not statistically significant, only for suppliers with few alternative customers. In Panel B, we restrict the sample to suppliers that produce highly specific goods (output-specific suppliers)—namely, suppliers with an above-the-median R&D to sales ratio. Within this sample, suppliers with few alternative customers display a stronger negative effect relative to the full sample of Panel A, but the effect of interest is still statistically insignificant. Finally, in Panel C, we further restrict the sample to the affected output-specific suppliers that provide goods and services to the subset of directly hit firms that themselves produce highly specific goods. Within this narrower sample, affected suppliers with few alternative customers display significantly lower profitability than similar firms in the control group. Overall, the results indicate that the upstream effect of the cyberattack is indeed rather limited, being concentrated among the subset of output-specific suppliers that provide goods and services to directly hit firms that produce highly specific goods and have few alternative customers.

5.3 Disruptions and Liquidity Risk Management

Next, we ask how the affected customers dealt with the decline in profits coming from the supply chain disruption. To pay their fixed and variable costs, affected customers may use their internal

[16] Following Barrot and Sauvagnat (2016), we define a directly hit firm as producing highly specific goods if its ratio of R&D expenditure to sales is above the median.

liquidity or increase their external borrowings. In Table 5, we estimate Equation (1) for the affected customers, using the liquidity ratio (current assets minus inventories divided by current liabilities) and the ratio of long-term debt to total assets as dependent variables.[17] Both ratios are multiplied by 100 for ease of interpretation of the estimates.

To sustain the negative effects of the cyberattack, affected customers relied on both internal liquidity and external borrowing. In Panel A, we estimate that affected customers reduce their liquidity ratio after the shock relative to control firms by about 0.3 percentage point, which corresponds to 30 percent of the sample median. In addition to relying on internal liquidity, affected customers increase external borrowing. In Panel B, we indeed find that affected customers increase long-term debt over total assets by about 1 percentage point relative to similar but unaffected firms. This effect is both statistically and economically significant, representing 13 percent of the median share of long-term debt to total assets.

Overall, we have found so far that the 2017 NotPetya cyberattack caused severe downstream supply chain disruptions, as affected customers saw significant declines in profitability. To cope with the shock, affected customers relied on both internal liquidity and external borrowing. While we exploit a shock exogenous to any given customer firm we analyze, to help validate our identification strategy we also show the coefficient plots of the difference-in-differences models in Figure 2. The parallel trends assumption seems to be validated by the lack of pre-trends for any of the outcome variables.

5.4 Disruptions and Bank Credit

We previously documented that affected customers increase their reliance on external financing to cope with the supply chain losses. Next, we focus on one of the most flexible ways in which firms can access external financing—namely, bank credit. To do so, we use confidential quarterly bank-borrower data from the Federal Reserve's Y-14 collection.[18] First, we test whether affected customers increase their borrowings from banks, in the form of either taking out new term loans

[17] The liquidity ratio measures the firm's ability to pay off current obligations with current assets.

[18] In unreported results, we confirm that our baseline effects are also present in the subsample of US firms.

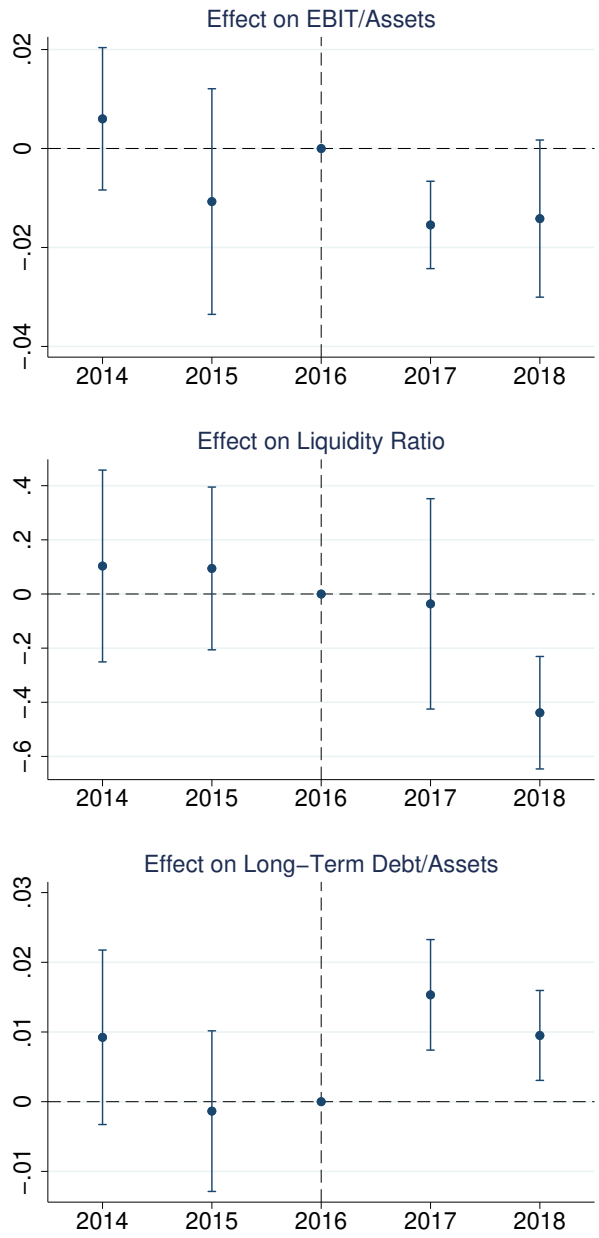

Figure 2: Parallel Trend Assumption, Coefficient Plots. This figure shows the estimated coefficients from the following specification: $Y_{ijt} = \alpha + \sum_{\tau=2014}^{2018} \beta_\tau \mathbb{I}_\tau \times \text{Affected}_i + \xi_i + \eta_{jt} + \epsilon_{it}$, where i is a firm and j is a country-year-industry-size bucket. Affected_i is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variables are EBIT/Assets, Liquidity Ratio, and Long-Term Debt/Assets. Standard errors are double clustered at the industry and country level. Source: BvD Orbis; FactSet Revere.

	(1)	(2)	(3)	(4)	(5)
PANEL A	Liquidity Ratio				
$Post_t \times Affected_i$	-0.156***	-0.201***	-0.291***	-0.255***	-0.225***
	(0.030)	(0.073)	(0.044)	(0.036)	(0.055)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.759	0.741	0.764	0.754	0.753
PANEL B	Long-Term Debt/Assets				
$Post_t \times Affected_i$	0.862***	1.357***	1.011**	1.468***	1.162***
	(0.125)	(0.384)	(0.393)	(0.352)	(0.393)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.880	0.867	0.884	0.882	0.882

Table 5: Effect on Customers' Financing. This table presents results from Equation (1). The sample period is 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in Panel A is the liquidity ratio, defined as 100 times current assets minus inventories, divided by current liabilities. The dependent variable in Panel B is long-term debt divided by assets—the ratio is multiplied by 100 for ease of interpretation of the point estimate. The indicator variable "Linked to Affected Industry" equals one for firms that have supply chain links to industries where directly hit firms operate. Standard errors are double clustered at the industry and country level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

or drawing down their credit lines. The results are reported in Table 6. Total committed credit (columns 1 and 2) and committed lines of credit (columns 3 and 4) remain unchanged. However, affected customers significantly increase credit line draw downs after the shock (columns 5 and 6), highlighting the importance of banks in the face of firms' immediate liquidity needs.[19]

Credit lines are short-term instruments that are often renewed at maturity. Since the affected customers in our study experience a decline in profitability and an increase in leverage, their credit

[19]These results are consistent with Brown, Gustafson, and Ivanov (2021) who, using the same data, show that firms respond to exogenous cash flow shocks (i.e., unexpectedly severe winter weather) by drawing down their credit lines at banks.

	(1)	(2)	(3)	(4)	(5)	(6)
	Log(Committed Credit)		Log(Committed CL)		Share Drawn Credit	
$Post_t \times Affected_i$	-0.069	0.047	-0.082	0.006	0.031***	0.042***
	(0.063)	(0.108)	(0.056)	(0.087)	(0.011)	(0.014)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Bank-Quarter	✓	✓	✓	✓	✓	✓
Industry-State-Quarter	✓		✓		✓	
Industry-State-Size Bucket-Quarter		✓		✓		✓
Observations	166,895	166,895	166,895	166,895	166,895	166,895
R-squared	0.624	0.629	0.641	0.643	0.607	0.625

Table 6: Effect on Bank Credit. This table presents results from Equation (2). The period of the firm-bank matched sample for the US is 2014:Q1 to 2018:Q4. $Post_t$ is a time dummy equal to one from 2017:Q3 onward. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variables are the logarithm of the total committed credit (committed line of credit and term loans) in columns (1)–(2), the logarithm of the committed line of credit in columns (3)–(4), and the share of the committed line of credit that is drawn down in columns (5)–(6). Standard errors are double clustered at the industry and bank level. *** p<0.01, ** p<0.05, * p<0.1. Source: Federal Reserve Y-14; FactSet Revere.

	(1)	(2)	(3)	(4)	(5)	(6)
	Share Drawn Credit		Share Drawn Credit		Interest Rate Spread	
$Post_t \times Affected_i \times CL\ Renewal_{ib}$	0.003	-0.002	-0.049	-0.044	0.127**	0.112**
	(0.025)	(0.023)	(0.050)	(0.039)	(0.048)	(0.050)
$Post_t \times Affected_i$	0.030**	0.042**	0.125***	0.126**	0.052	0.000
	(0.012)	(0.017)	(0.039)	(0.054)	(0.090)	(0.064)
$Post_t \times CL\ Renewal_{ib}$	0.006	0.009	0.001	0.003	-0.026	-0.014
	(0.007)	(0.006)	(0.010)	(0.009)	(0.017)	(0.016)
$Affected_i \times CL\ Renewal_{ib}$	-0.002	0.000	0.004	0.016	-0.064	-0.063
	(0.021)	(0.021)	(0.033)	(0.035)	(0.053)	(0.052)
$CL\ Renewal_{ib}$	0.001	0.001	0.005	0.004	0.063	0.059
	(0.006)	(0.006)	(0.010)	(0.010)	(0.039)	(0.040)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Bank-Quarter	✓	✓	✓	✓	✓	✓
Industry-State-Quarter	✓		✓		✓	
Industry-State-Size Bucket-Quarter		✓		✓		✓
Observations	166,895	166,895	91,369	91,369	91,369	91,369
R-squared	0.607	0.625	0.577	0.595	0.722	0.734

Table 7: Effect on Bank Credit Line Drawdowns and Interest Rates. This table presents coefficient estimates of Equation (4). The period of the firm-bank matched sample for the US is 2014:Q1 to 2018:Q4. $Post_t$ is a time dummy equal to one from 2017:Q3 onward. $CLRenewal_{ib}$ is an indicator variable equal to one if firm i has a credit line with bank b that was renewed after the shock, and zero otherwise. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variables are the share of the committed line of credit that is drawn down in columns (1)–(4) and the interest rate spread in columns (5)-(6). We use the full sample in columns (1)–(2) and the subsample with non-missing interest rate data in columns (3)–(6). Standard errors are double clustered at the industry and bank level. *** p<0.01, ** p<0.05, * p<0.1. Source: Federal Reserve Y-14; FactSet Revere.

lines at banks could have been renewed at less attractive terms after the cyberattack. We investigate this hypothesis by examining the heterogeneous response of credit line drawdowns and interest rate spreads to the shock, depending on whether borrower i renewed a credit line with a given bank b during the post-shock period (2017:Q3–2018:Q4). Specifically, we expand our baseline loan-level specification as follows:

$$Y_{ibjt} = \alpha + \beta_1 \text{Post}_t \times \text{Affected}_i \times \text{CL Renewal}_{ib} + \beta_2 \text{Post}_t \times \text{Affected}_i + \beta_3 \text{Post}_t \times \text{CL Renewal}_{ib} + \beta_4 \text{Affected}_i \times \text{CL Renewal}_{ib} + \beta_5 \text{CL Renewal}_{ib} + \xi_i + \eta_{jt} + \gamma_{bt} + \epsilon_{ibjt} \quad (4)$$

where CL Renewal_{ib} is a time-invariant dummy variable equal to one if firm i has a credit line with bank b that was renewed after the shock, and zero otherwise. As before, Affected_i is absorbed by firm fixed effects, and Post_t is absorbed by time fixed effects.

The results are reported in Table 7. Affected customers draw down their credit lines after the shock at similar rates irrespective of whether their credit lines are renewed after the cyberattack. This result holds both in the full sample (columns 1–2) and in the subsample with available interest rate spread information (columns 3–4). However, in line with our hypothesis, the increase in interest rates spreads is concentrated among affected customers with credit line renewals soon after the shock (columns 5 and 6). These findings indicate that affected customers significantly draw down their credit lines to cope with the pressing liquidity needs arising from the supply chain disruption. However, this adjustment comes at a cost, since banks charge higher interest rates to the affected customers that have to renew their credit lines soon after the shock.[20]

Overall, affected customers experience a significant drop in profitability but are able to withstand the supply chain shock by using both internal liquidity and external sources of financing. Albeit of large magnitude, our shock is nevertheless temporary and occurred during an economic expansion and stable financial conditions. As a result, we do not expect to observe significant changes in employment and investment among the affected customers. This is indeed what we find in Table A.10 of the Online Appendix. Using the same difference-in-differences setup of Equation (1), columns

[20] In Table A.9 of the Online Appendix, we also test whether banks revise additional credit terms for the affected customers relative to the control group, including the amount of collateral requested and the maturity of the committed exposure, and find no significant effects.

(1)–(3) reveal that affected customers display similar growth in the number of employees after the shock relative to firms in the control group. Similarly, columns (4)–(6) show that the effect of supply chain disruptions on customers' investment in tangible assets is insignificant. In short, together with the increased reliance on internal liquidity, access to external finance allows affected customers to absorb the loss in profitability coming from the supply chain shock without having to cut either employment or investment.

5.5 Disruptions and Dynamic Supply Chain Responses

As the NotPetya cyberattack exposed firms to the possibility that a supplier could stop operations for several weeks, in this final section we test whether there are persistent changes to the supply chain network of affected customers after the shock.

We start by examining whether affected customers are more likely to terminate trading relationships with the directly hit suppliers. We proceed in two different ways based on the choice of the control group. First, we compare the behavior of affected customers with that of otherwise similar firms, as in Equation (1). Since, by construction, firms in the control group do not have relations with directly hit firms, they cannot terminate them either. Therefore, we estimate the desired effect in two steps. We first use a dependent variable (Terminated Relations) that counts the number of relations ended by affected customer i with any supplier in the same industry k as the directly hit supplier s. Then we use a second dependent variable (Terminated Relations excl. Hit Supplier) that counts the number of relations that affected customer i terminates with suppliers other than the directly hit one, in the same affected industry k. As a result, the difference between the two estimates can be attributed to affected customers ending trading relations with the directly hit supplier. In both cases, the count of relations ended by firms in the control group is limited to the suppliers in the affected industries. Since we are interested in highlighting the dynamic supply chain adjustments, we estimate the immediate response which happened within six months from the attack (Post_{2017}) separately from the medium-term response, which occurred more than one year after the attack (Post_{2018}).

Second, we examine the termination of relations by comparing, within affected customers, the likelihood of terminating the relation with a directly hit supplier with the likelihood of terminating

a relation with another supplier in the same industry. To this purpose, we focus on the cross-section of customer-supplier relations and estimate the following linear probability model:

$$Terminated(t)_{is} = \alpha + \beta DirectlyHitSupplier_s + \eta_{ik} + \epsilon_{is} \tag{5}$$

where i identifies the subset of affected customers and s the different suppliers of each customer. Terminated(t)$_{is}$ equals one if a relation that existed at the time of the shock (June 2017) between customer i and supplier s is terminated after the shock—either in year t=2017 (July to December) or in year t=2018. $DirectlyHitSupplier_s$ equals one if supplier s is directly hit by the cyberattack. Since we want to estimate the likelihood that a customer terminates the relation with a directly hit supplier relative to the likelihood of terminating one with an alternative supplier, we also include in the model the fixed effects η_{ik}, which correspond to the interaction of the affected customer identifier with the industry of the supplier, country of the supplier, and size quartile of the supplier at the time of the shock.

The results are reported in Table 8. In columns (1)–(2), we consider the number of terminated relationships with any supplier in the same industry as the directly hit supplier. Specifically, the dependent variable is the logarithm of one plus the number of ended relations. In contrast, in columns (3)–(4), the dependent variable is the logarithm of one plus the number of relations ended with all suppliers except the directly hit one. The coefficient of Post$_{2017}\times$ Affected$_i$ is virtually the same in columns (2) and (4), indicating that affected customers do not immediately end relations with the directly hit suppliers or any other supplier. However, affected customers are more likely to terminate relations with the directly hit suppliers in the medium-term. Indeed, the coefficient of Post$_{2018}\times$ Affected$_i$ is positive and statistically significant in column (2) when considering all suppliers and statistically and economically insignificant in column (4) when considering all suppliers except for the directly hit one. Then, in columns (5)–(6), we carry out a different test that exploits variation within the set of affected customers. Column (5) suggests that in 2017 affected customers are as likely to terminate the relation with the directly hit supplier as with any other alternative supplier. Only in 2018 do we observe that affected customers are more likely to terminate the relation with the directly hit firm than with any other alternative supplier. This finding is consistent with the results of columns (1)–(4).

Next, we examine whether affected customers build new trading relations with alternative suppliers

	(1)	(2)	(3)	(4)	(5)	(6)
	Terminated Relations		Terminated Relations excl. Hit Supplier		Terminated Relations in 2017	in 2018
$\text{Post}_{2017} \times \text{Affected}_i$	0.051	0.024	0.035	0.016		
	(0.043)	(0.044)	(0.049)	(0.048)		
$\text{Post}_{2018} \times \text{Affected}_i$	0.199***	0.145**	0.067	0.016		
	(0.065)	(0.070)	(0.075)	(0.071)		
Directly Hit Supplier					0.031	0.058**
					(0.019)	(0.024)
Fixed Effects						
Firm	✓	✓	✓	✓		
Country-Size Bucket-Linked to Affected Industry-Year	✓		✓			
Industry-Size Bucket-Linked to Affected Industry-Year		✓		✓		
Customer-Industry Supplier-Country Supplier-Size Bucket Supplier					✓	✓
Unit of observation	firm-year	firm-year	firm-year	firm-year	firm-supplier	firm-supplier
Observations	45,583	45,886	45,583	45,886	13,431	13,431
R-squared	0.667	0.671	0.664	0.668	0.135	0.068

Table 8: Effect on Terminated Relations. This table presents results from Equation (1) in columns (1)–(4) and Equation (5) in columns (5)–(6). In columns (1)–(4), the sample period is 2014 to 2018; $Post_{2017}$ is a time dummy equal to one in 2017; $Post_{2018}$ is a time dummy equal to one in 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in columns (1)-(2) is the logarithm of (one plus) relations ended in year t with firms in the same industry (SIC2) of the directly hit firm. The dependent variable in columns (3)–(4) is the logarithm of (one plus) relations ended in year t with firms in the same industry (SIC2) of the directly hit firm, excluding those ended with the directly hit firm. In columns (5)–(6), the sample is a cross section at the customer-supplier level and contains only affected customers. Terminated in 2017 (2018) equals one if a relationship that existed at the time of the shock between a customer and its supplier is terminated in year 2017 (2018), and zero if it continues; DirectlyHitSupplier equals one if a supplier is directly hit by the cyberattack. Standard errors are double clustered at the industry and country level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

after the cyberattack. Consider affected customer i, which is exposed to the shock because of its connection with directly hit supplier s, which operates in industry k. For this treated firm i, we count the number of new relationships formed after the cyberattack with suppliers in industry k. For the control group to provide a reliable benchmark, we also compute the number of new relations that control firm c (which belongs to the same industry/country and size quartile as affected customer firm i) has with suppliers in the same industry k. We repeat this process for each firm c in the control group. This procedure effectively requires firm c in the control group not only to be in the same industry (or country) and size quartile as affected customer i, but also to have a supplier in the same industry k as the directly hit supplier s of affected customer i.

The results are displayed in Table 9, columns (1)–(2). The dependent variable is the logarithm of one plus the number of new relations (in the same industry as the directly hit supplier). Estimates indicate that affected customers significantly increased the number of new alternative suppliers soon after the cyberattack. The point estimate suggests that affected customers have 13 to 15% more new alternative suppliers than firms in the control group within six months after the cyberattack. Instead, the differential change in the number of new relations in 2018 is small and not significant at the 5 percent level.

Finally, in columns (3)–(8), we explore whether the composition of the new supplier network is significantly different from the pre-shock one for affected customers relative to otherwise similar firms. While we do not observe a significant change in either geography or size of the suppliers' network for affected customers after the cyberattack (columns 3–6), we show that there is a significant reduction in the cybersecurity risk exposure of the suppliers of affected customers relative to the suppliers of otherwise similar firms, as measured by Florakis, Louca, Michaely, and Weber (2022) (columns 7–8).

Overall, the evidence presented in Table 8 and Table 9 suggests that affected customers are likely to take immediate steps to form new trading relationships with alternative suppliers and later terminate those with the suppliers that caused the disruption. This dynamic adjustment can be explained by customers preferring to trade with a new supplier before they stop trading with the old one in order not to interrupt production. Moreover, the new suppliers of the affected customers tend to be, on net, less exposed to cybersecurity risk, suggesting that the temporary disruptions caused by the cyberattack had long-lasting effects by eroding the reputation of the directly hit firms as reliable suppliers. In fact, reliability and timeliness are essential for the smooth functioning of the

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	New Relations		Domestic Suppliers (%)		Suppliers' Size		Suppliers' Cyber Risk	
$Post_{2017} \times Affected_i$	0.150**	0.128**						
	(0.064)	(0.057)						
$Post_{2018} \times Affected_i$	0.001	-0.047*						
	(0.023)	(0.025)						
$Post \times Affected_i$			-0.011	-0.017	0.040	0.025	-0.028***	-0.025*
			(0.010)	(0.011)	(0.057)	(0.057)	(0.011)	(0.013)
Fixed Effects								
Firm	✓	✓	✓	✓	✓	✓	✓	✓
Country-Size Bucket-Linked to Affected Industry-Year	✓		✓		✓		✓	
Industry-Size Bucket-Linked to Affected Industry-Year		✓		✓		✓		✓
Sample	Full	Full	Full	Full	Full	Full	US firms	US firms
Observations	45,583	45,886	36,722	36,973	36,722	36,973	4,789	4,456
R-squared	0.695	0.696	0.814	0.818	0.805	0.806	0.764	0.808

Table 9: Effect on New Relations and Suppliers Composition. This table presents results from Equation (1). The sample period is 2014 to 2018. $Post_{2017}$ is a time dummy equal to one in 2017. $Post_{2018}$ is a time dummy equal to one in 2018. *Post* is a time dummy equal to one in 2017 and 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in columns (1)–(2) is the logarithm of (one plus) relations started in year t with firms in the same industry (SIC2) of the directly hit firm. The dependent variable in columns (3)–(4) is the share of firms' suppliers that are located in the same country of the firm. The dependent variable in columns (5)–(6) is the logarithm of the median assets of firms' suppliers. The dependent variable in columns (7)–(8) is the asset-weighted average cyber risk of the firms' suppliers. The cyber risk measure is from Florakis et al. (2022) and is only available for US listed firms. Standard errors are double clustered at the industry and country level in columns (1)–(6) and clustered at the industry level in columns (7)–(8). *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

now widely used "just-in-time" production systems (Crémer, 1995). The cyberattack also prompted affected customers to search for suppliers with a stronger cybersecurity posture, likely leading to a more cyber-resilient supply chain.

6 Conclusion

We study the supply chain effects of the most damaging cyberattack in history. Originated by Russian military intelligence to hit the Ukrainian economy, the virus also infected Ukrainian subsidiaries of international companies and spread to their global network infrastructure, thus forcing them to halt operations for several weeks. As a result, the customers of these directly hit firms recorded significantly lower profits relative to similar but unaffected firms. To cope with the shock, affected customers used their internal liquidity and increased borrowing, mainly by drawing down their credit lines with banks. This increased reliance on internal liquidity and external finance allowed affected customers to absorb the losses without having to reduce either employment or investment.

We also document how the severity of the downstream disruption depended on the vulnerability of the supply chain. Specifically, we show that affected customers with fewer alternative suppliers that could substitute for the directly hit one experienced larger drops in profitability. This result highlights the importance of building more resilient supply chains to mitigate the effects of disruptive cyberattacks as well as other shocks, including the COVID-19 pandemic. Finally, we uncover evidence consistent with the fact that affected customers build new trading relations with alternative suppliers immediately after the cyberattack and subsequently terminate relations with the suppliers responsible for the disruption in the medium term. In addition, the new supplier network appears to be more cyber-resilient.

Our paper has several policy implications. First, our results show the crucial need for better cybersecurity, including more compartmentalization of the network infrastructure, more scrutiny on the cybersecurity of third-party suppliers, and at least one backup facility that is offline at any time. For instance, Maersk's Ghana office happened to be offline due to a blackout and, thanks only to that, Maersk was able to restore its networks (Greenberg, 2019). Second, firms need to improve their risk management and contingency planning, with the goal of continuing activities in the event that anyone of their suppliers is unable to provide goods and services. The resilience of a supply chain

rests on having multiple options for each intermediate good or service so that no single supplier is irreplaceable (Elliott, Golub, and Leduc, 2022). Third, the intelligence community should establish credible deterrence for cyber-aggressions of the magnitude of NotPetya so that state-sponsored hackers at least have an incentive to put in place controls to make sure that the attack does not spread beyond its intended reach. For instance, even though Stuxnet allegedly infected more than 100,000 computers worldwide, it did not do any damage outside of its target of Iranian industrial control systems engaged in enriching uranium.

References

Accenture, 2019. The cost of cybercrime. Accenture.

Acemoglu, D., Akcigit, U., Kerr, W., 2016. Networks and the macroeconomy: An empirical exploration. NBER Macroeconomics Annual 30, 273–335.

Akey, P., Lewellen, S., Liskovich, I., Schiller, C., 2021. Hacking corporate reputations. Working Paper.

Aldasoro, I., Gambacorta, L., Giudici, P., Leach, T., 2022. The drivers of cyber risk. Journal of Financial Stability 60, 100989.

Alfaro, L., García-Santana, M., Moral-Benito, E., 2021. On the direct and indirect real effects of credit supply shocks. Journal of Financial Economics 139 (3), 895–921.

Amir, E., Levi, S., Livne, T., 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies 23 (3), 1177–1206.

Barrot, J.-N., Sauvagnat, J., 2016. Input specificity and the propagation of idiosyncratic shocks in production networks. Quarterly Journal of Economics 131 (3), 1543–1592.

Boehm, C. E., Flaaen, A., Pandalai-Nayar, N., 2019. Input linkages and the transmission of shocks: firm-level evidence from the 2011 Tōhoku earthquake. Review of Economics and Statistics 101 (1), 60–75.

Brown, J. R., Gustafson, M., Ivanov, I., 2021. Weathering cash flow shocks. Journal of Finance 76 (4), 1731–1772.

Carvalho, V. M., Nirei, M., Saito, Y. U., Tahbaz-Salehi, A., 2021. Supply chain disruptions: Evidence from the Great East Japan earthquake. Quarterly Journal of Economics 136 (2), 1255–1321.

Cortes, G. S., Silva, T. C., Van Doornik, B. F., 2019. Credit shock propagation in firm networks: Evidence from government bank credit expansions. Working Paper.

Costello, A. M., 2020. Credit market disruptions and liquidity spillover effects in the supply chain. Journal of Political Economy 128 (9), 3434–3468.

Crémer, J., 1995. Towards an economic theory of incentives in just-in-time manufacturing. European Economic Review 39 (3-4), 432–439.

Demir, B., Javorcik, B., Michalski, T. K., Ors, E., 2022. Financial constraints and propagation of shocks in production networks. Review of Economics and Statistics, forthcoming.

Duffie, D., Younger, J., 2019. Cyber runs. Working Paper.

Eisenbach, T. M., Kovner, A., Lee, M. J., 2021. Cyber risk and the US financial system: A pre-mortem analysis. Journal of Financial Economics, forthcoming.

Elliott, M., Golub, B., Leduc, M. V., 2022. Supply network formation and fragility. American Economic Review, forthcoming.

Florakis, C., Louca, C., Michaely, R., Weber, M., 2022. Cybersecurity risk. Review of Financial Studies, forthcoming.

Garg, P., 2020. Cybersecurity breaches and cash holdings: Spillover effect. Financial Management 49 (2), 503–519.

Gofman, M., Segal, G., Wu, Y., 2020. Production networks and stock returns: The role of vertical creative destruction. Review of Financial Studies 33 (12), 5856–5905.

Greenberg, A., 2018. The untold story of NotPetya, the most devastating cyberattack in history. Wired.

Greenberg, A., 2019. Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Doubleday.

Jamilov, R., Rey, H., Tahoun, A., 2021. The anatomy of cyber risk. Working Paper.

Kalemli-Ozcan, S., Sørensen, B. E., Villegas-Sanchez, C., Volosovych, V., Yesiltas, S., 2022. How to construct nationally representative firm level data from the ORBIS global database. Working Paper.

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

Kashyap, A. K., Wetherilt, A., 2019. Some principles for regulating cyber risk. AEA Papers and Proceedings 109, 482–87.

Kotidis, A., Schreft, S. L., 2022. Cyberattacks and financial stability: Evidence from a natural experiment. FEDS Working Paper No. 2022-025 .

Moody's, 2020. Suppliers and vendors are becoming the weakest link in corporate cybersecurity. Moody's.

Ozdagli, A., Weber, M., 2021. Monetary policy through production networks: Evidence from the stock market. Working Paper.

Powell, J., 2021. 60 minutes interview transcript. CBS.

Siemens, 2019. Caught in the crosshairs: Are utilities keeping up with the industrial cyber threat?. Siemens.

US Congress, 2021. House hearing, 117th Congress - Homeland cybersecurity: Assessing cyber threats and building resilience. Committee on Homeland Security.

Verizon, 2019. Data breach investigations report. Verizon.

WEF, 2019. Regional risks for Doing Business 2019. World Economic Forum.

Welburn, J. W., Strong, A. M., 2021. Systemic cyber risk and aggregate impacts. Risk Analysis, forthcoming.

Online Appendix

A.1 Variables Description

Age is the difference, in years, between the current year and the incorporation year of the firm.
Assets are total assets (BvD code TOAS) in millions of USD.
EBIT/Assets is the operating profit/loss (BvD code OPPL) divided by total assets.
Liquidity Ratio is calculated as 100*((current assets − inventories)/ current liabilities). The BvD code is LIQR.
LT Debt/Assets is long-term debt (maturity greater than one year) divided by total assets, multiplied by 100. The BvD code is LTDB.
ROA is (profit (loss) for period / total assets) * 100. The BvD code is ROA.
No. employees is the number of employees (BvD code EMPL).
Cost of Employees/Assets is the cost of employees divided by assets. The BvD code is STAF.
Tang. Fixed. Assets/Assets is tangible fixed assets/assets. The BvD code is TFAS.
Affected is a dummy equal to one if the firm is a supplier (customer) of a directly hit firm.
Commitment Amount is defined as the sum of credit line commitments and term loan amounts.
Utilized Amount is defined as the sum of credit line drawdowns and term loan amounts.
Maturity is the weighted average remaining maturity of all commitments to a given borrower, where the weights are proportional to the loan commitment amounts of each of the borrower's loans.
Terminated Relations is the log of (one plus) relations ended in t with firms in the same SIC2 of the directly hit firm.
New Relations is the log of (one plus) relations started t with firms in the same SIC2 of the directly hit firm.
DirectlyHitSupplier equals one if a supplier is directly hit by the cyberattack.
Domestic Suppliers is the share of firms' suppliers that located in the same country of the firm.
Suppliers' Size is the logarithm of the median assets of firms' suppliers.
Suppliers' Cyber Risk is the asset-weighted average cyber risk of the firms' suppliers.

A.2 Additional Figures

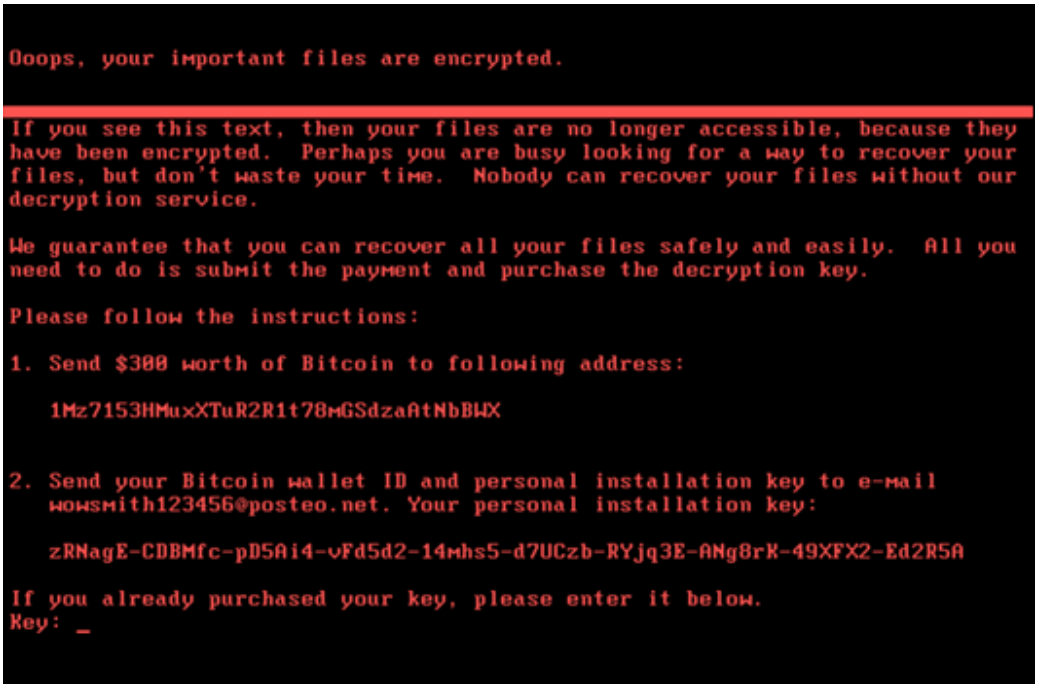

Figure A.1: Computer Screen after NotPetya Infection. This figure shows the screen of a computer infected by NotPetya. It resembled a ransomware as it asked for a Bitcoin payment to obtain the decryption key. Source: www.crowdstrike.com.

Figure A.2: Geographical Location of Directly Hit Firms. This figure shows the geographical distribution of directly hit firms. Darker green colors indicate a larger mass of directly hit firms. Source: Orbis; FactSet Revere.

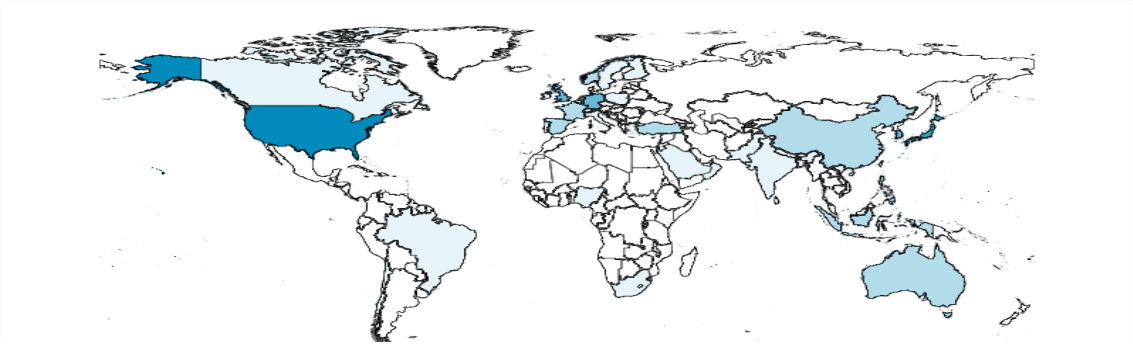

Figure A.3: Geographical Location of Affected Customers. This figure shows the geographical distribution of affected customers. Darker colors indicate a larger mass of affected customers. Source: Bvd Orbis; FactSet Revere.

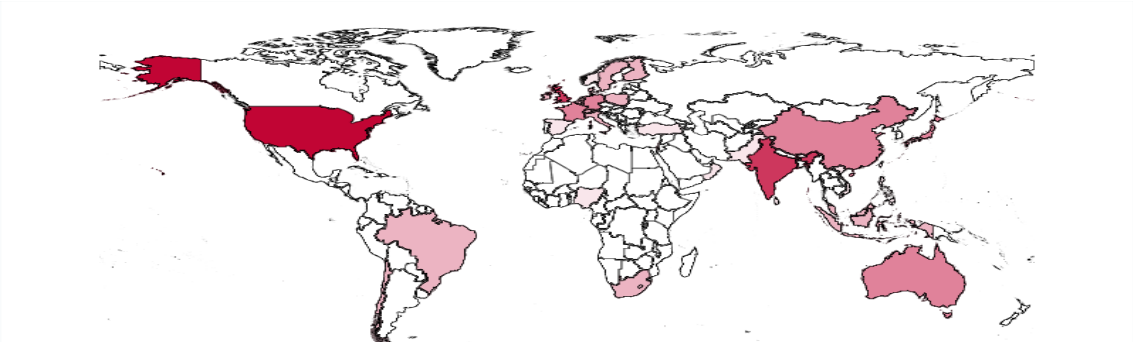

Figure A.4: Geographical Location of Affected Suppliers. This figure shows the geographical distribution of affected suppliers. Darker colors indicate a larger mass of affected suppliers. Source: Orbis; FactSet Revere.

A.3 Additional Tables

SIC Industry Division	No. Directly Hit Firms	No. Customers	No. Suppliers
Manufacturing	4	130	146
Services	2	23	90
Transportation, Communications, Electric, Gas, and Sanitary Services	2	43	57
Agriculture, Forestry, and Fishing	0	1	1
Construction	0	1	4
Mining	0	4	7
Retail Trade	0	19	7
Wholesale Trade	0	12	8
Total	8	233	320

Table A.1: Number of Directly Hit Firms, Customers, and Suppliers, by Industry. This table shows the number of unique directly hit firms, customers, and suppliers in our sample by SIC industry divison. Source: BvD Orbis; FactSet Revere.

		Full	Size Q1		Size Q2		Size Q3		Size Q4	
	Stat	Sample	Treated	Control	Treated	Control	Treated	Control	Treated	Control
No. Obs.	Tot	70590	355	20792	357	20767	356	17539	360	10064
Age	μ	32.84	21.39	27.42	25.87	33.24	34.26	34.79	36.69	40.32
	p(50)	24.00	18.00	22.00	21.00	24.00	26.00	24.00	24.00	27.00
	σ	26.95	12.69	21.18	19.43	25.73	31.03	28.49	34.00	34.09
Assets (M)	μ	3718	102	92	443	436	1807	1838	34193	20481
	p(50)	498	101	85	424	400	1575	1603	10676	9344
	σ	15673	56	58	177	172	855	871	70262	34275
EBIT/Assets	μ	0.04	-0.02	-0.02	0.04	0.05	0.06	0.06	0.07	0.06
	p(50)	0.05	0.03	0.04	0.06	0.05	0.06	0.06	0.06	0.06
	σ	0.17	0.24	0.27	0.13	0.11	0.07	0.08	0.06	0.07
Liquidity Ratio	μ	1.95	3.28	2.73	1.86	1.92	1.41	1.47	1.40	1.21
	p(50)	1.24	1.70	1.59	1.33	1.29	1.08	1.13	0.99	0.98
	σ	3.02	5.50	4.28	2.61	2.84	1.44	1.59	1.47	1.11
LT Debt/Assets	μ	12.95	6.64	6.78	13.95	10.21	23.98	17.04	24.56	23.60
	p(50)	7.64	1.18	1.16	8.70	4.82	22.72	13.33	23.54	21.99
	σ	15.05	9.75	11.13	16.89	13.27	16.54	16.04	15.87	15.53
ROA	μ	1.78	-3.90	-2.10	0.70	3.01	3.11	3.76	3.67	3.82
	p(50)	3.35	1.93	2.59	3.31	3.58	3.48	3.63	3.39	3.37
	σ	12.99	21.51	19.17	12.97	10.40	7.40	7.64	5.60	5.81
No. Employees	μ	9679	689	679	2053	2438	7483	7403	57121	39459
	p(50)	1968	402	331	1248	1413	4655	4502	18065	18031
	σ	31110	1213	1535	2084	5036	10693	11244	96856	64499
Cost of Employees/Assets	μ	0.14	0.20	0.19	0.16	0.14	0.12	0.11	0.10	0.09
	p(50)	0.09	0.11	0.13	0.08	0.08	0.07	0.06	0.07	0.05
	σ	0.20	0.27	0.24	0.19	0.17	0.13	0.15	0.11	0.20
Tang. Fixed Assets/Assets	μ	0.28	0.17	0.22	0.25	0.28	0.33	0.31	0.25	0.35
	p(50)	0.23	0.09	0.17	0.18	0.24	0.26	0.26	0.16	0.31
	σ	0.23	0.19	0.20	0.22	0.22	0.25	0.23	0.23	0.25

Table A.2: Summary Statistics, Treated versus Control Suppliers. This table shows summary statistics for our sample firms. The table reports mean, median, and standard deviation. The sample period is 2014 to 2018. The table shows the summary statistics for the full sample as well as the summary statistics for treated and control firms in each of the four size bucket groups. Treated firms are suppliers of a directly affected firm. Age is in years. Assets are in millions of USD. The liquidity ratio is 100*(current assets – inventories)/current liabilities. Long-term debt (LT Debt) is financial debt with a maturity greater than one year. All the variables divided by total assets (A) are expressed as ratios. However, for ease of interpretation of the estimates, LT Debt/A is multiplied by 100. Source: BvD Orbis; FactSet Revere.

		Full	Size Q1		Size Q2		Size Q3		Size Q4	
	Stat	Sample	Treated	Control	Treated	Control	Treated	Control	Treated	Control
No. Obs.	Tot	42778	161	31039	162	8642	161	1981	164	468
Age	μ	31.83	26.87	29.83	35.75	35.79	49.39	40.93	52.66	39.68
	p(50)	23.00	20.00	22.00	28.00	24.00	30.00	29.00	35.50	28.00
	σ	26.84	22.31	24.24	27.27	31.13	46.12	33.68	43.72	33.40
Assets (M)	μ	3493	534	394	4853	3864	24461	19526	128540	83861
	p(50)	466	389	259	4708	3071	23146	16995	108312	66081
	σ	14854	432	379	2505	2209	10060	8156	84634	58666
EBIT/Assets	μ	0.04	0.01	0.02	0.06	0.06	0.08	0.06	0.06	0.06
	p(50)	0.05	0.07	0.05	0.06	0.06	0.07	0.05	0.06	0.05
	σ	0.17	0.24	0.19	0.08	0.08	0.07	0.06	0.05	0.06
Liquidity Ratio	μ	1.95	3.10	2.19	1.68	1.37	1.07	1.16	1.30	1.00
	p(50)	1.24	1.74	1.36	1.18	1.08	0.88	0.96	0.93	0.90
	σ	3.02	4.33	3.44	1.95	1.34	0.64	1.32	1.52	0.64
LT Debt/Assets	μ	12.95	7.16	9.76	21.51	20.67	21.96	25.18	21.44	24.88
	p(50)	7.64	1.99	3.90	19.14	18.47	21.56	23.53	20.91	23.62
	σ	15.05	11.14	13.27	17.36	16.43	13.4401	15.52	11.84	12.93
ROA	μ	1.66	-0.36	0.97	3.17	3.57	5.26	3.28	4.64	3.29
	p(50)	3.27	5.45	3.24	3.82	3.46	4.47	2.84	4.30	2.71
	σ	13.02	21.21	14.58	6.93	7.12	5.42	5.75	5.49	5.18
No. Employees	μ	9499	2711	2255	15870	13985	69098	45436	124827	97873
	p(50)	1895	1290	984	8969	7635	43320	26400	97900	62454
	σ	30539	3408	4445	20415	31063	72122	61184	94473	96951
Cost of Employees/Assets	μ	0.15	0.13	0.16	0.08	0.11	0.12	0.08	0.09	0.05
	p(50)	0.09	0.10	0.10	0.05	0.06	0.11	0.04	0.06	0.04
	σ	0.21	0.13	0.21	0.10	0.21	0.08	0.14	0.07	0.05
Tang. Fixed Assets/Assets	μ	0.28	0.22	0.26	0.25	0.33	0.29	0.38	0.24	0.39
	p(50)	0.23	0.17	0.22	0.16	0.28	0.23	0.35	0.20	0.36
	σ	0.23	0.19	0.22	0.21	0.24	0.21	0.26	0.19	0.26

Table A.3: Summary Statistics, Treated versus Control Customers, Pre-Period. This table shows summary statistics for our sample firms. The table reports mean, median, and standard deviation. The sample period is 2014 to 2016. The table shows the summary statistics for the full sample as well as the summary statistics for treated and control firms in each of the four size bucket groups. Treated firms are customers of a directly affected firm. Age is in years. Assets are in millions of USD. The liquidity ratio is 100*(current assets – inventories)/current liabilities. Long-term debt (LT Debt) is financial debt with a maturity greater than one year. All the variables divided by total assets (A) are expressed as ratios. However, for ease of interpretation of the estimates, LT Debt/A is multiplied by 100. Source: BvD Orbis; FactSet Revere.

	(1)	(2)	(3)	(4)	(5)
PANEL A: Continuous Variable			EBIT/Assets		
$Post_t \times \widetilde{Affected}_i$	-1.219***	-1.648***	-1.843***	-1.993***	-1.778***
	(0.378)	(0.566)	(0.674)	(0.617)	(0.659)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748
PANEL B: Alternative Clustering			EBIT/Assets		
$Post_t \times Affected_i$	-0.010*	-0.012**	-0.013*	-0.015***	-0.012**
	(0.005)	(0.005)	(0.008)	(0.005)	(0.006)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748

Table A.4: Effect on Profitability of Customers—Robustness. This table presents results from Equation (1). The sample period is 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. In Panel A, $\widetilde{Affected}_i$ is a variable equal to the reported costs suffered by the directly hit firms shown in Table 1 normalized by their respective total assets if firm i is a customer of a directly hit firm. In Panel B, $Affected_i$ is a dummy equal to one if firm i is a customer of a directly hit firm. The dependent variable is EBIT divided by assets. In Panel A, standard errors are double clustered at the industry and country level. In Panel B, standard errors are clustered at the industry-upstream industry level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

	(1)	(2)	(3)
	EBIT/Assets		
$\text{Post}_t \times$ Affected(2D)$_i$	0.002	0.000	0.000
	(0.002)	(0.002)	(0.002)
Fixed Effects			
Firm	✓	✓	✓
Country-Industry-Year	✓		
Size Bucket-Industry-Year		✓	
Size Bucket-Industry-Country-Year			✓
Observations	63,859	67,458	57,829
R-squared	0.757	0.742	0.772

Table A.5: Effect on Profitability, Customers of Affected Customers. This table presents results from Equation (1). The sample period is 2014 to 2018. Affected(2D)$_i$ is a dummy equal to one if firm i is a customer of a customer of a directly hit firm. The dependent variable is EBIT divided by assets. Standard errors are clustered at the industry level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

	(1)	(2)	(3)	(4)	(5)
			EBIT/Assets		
$\text{Post}_t \times \text{Affected}_i \times \mathbb{1}(\text{Suppliers}<5)_i$	-0.046***	-0.042***	-0.048**	-0.039**	-0.038**
	(0.014)	(0.015)	(0.020)	(0.017)	(0.017)
$\text{Post}_t \times \mathbb{1}(\text{Suppliers}<5)_i$	0.005**	0.003	0.005**	-0.001	-0.004
	(0.002)	(0.002)	(0.002)	(0.004)	(0.004)
$\text{Post}_t \times \text{Affected}_i$	0.008*	0.008*	0.008	0.003	0.004
	(0.005)	(0.004)	(0.009)	(0.009)	(0.007)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,309	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748

Table A.6: Effect on Customers' Profitability, Difference-in-Differences. This table presents results from the following difference-in-differences model: $Y_{ijt} = \alpha + \beta_1 \text{Post}_t \times \text{Affected}_i \times \mathbb{1}(\text{Suppliers} < 5)_i + \beta_2 \text{Post}_t \times \mathbb{1}(\text{Suppliers} < 5)_i + \beta_3 \text{Post}_t \times \text{Affected}_i + \xi_i + \eta_{jt} + \epsilon_{ijt}$. The sample period is 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. $\textit{Affected}_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable is EBIT divided by assets. The indicator variable $\mathbb{1}(\text{Suppliers} < 5)_i$ is equal to one if, at the time of the shock (July 2017), firm i has four or less alternative suppliers (if firm i is treated) or an average of four or less suppliers in an affected industry (if firm i is in the control group). The indicator variable "Linked to Affected Industry" equals one for firms that have supply chain links to industries where directly hit firms operate. Standard errors are double clustered at the industry and country level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

	(1)	(2)	(3)	(4)	(5)
	EBIT/Assets				
$Post_t \times Affected_i \times Specific_i$	-0.017**	-0.020**	-0.022*	-0.024**	-0.020**
	(0.007)	(0.009)	(0.013)	(0.011)	(0.010)
$Post_t \times Affected_i \times NotSpecific_i$	-0.005*	-0.006	-0.006	-0.009**	-0.007
	(0.003)	(0.005)	(0.004)	(0.005)	(0.005)
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓
Observations	66,225	69,827	62,311	45,583	45,886
R-squared	0.757	0.740	0.762	0.745	0.748

Table A.7: Effect on Customers' Profitability, Heterogeneity across Product Specificity. This table presents results from Equation (3). The sample period is 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable is EBIT divided by assets. The variable Specific (NotSpecific) equals one for the affected customers linked to directly hit firms with an above-the-median (below-the-median) R&D-to-sales ratio. Standard errors are double clustered at the industry and country level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

	(1)	(2)	(3)	(4)	(5)
Panel A: Full Sample			EBIT/Assets		
$\text{Post}_t \times \text{Affected Supplier}_i \times \mathbb{1}(\text{Customers}<5)_i$	-0.008	-0.005	-0.010*	-0.004	-0.005
	(0.007)	(0.007)	(0.006)	(0.005)	(0.007)
$\text{Post}_t \times \text{Affected Supplier}_i \times \mathbb{1}(\text{Customers}\geq 5)_i$	0.005	0.002	0.005	0.008	0.003
	(0.011)	(0.008)	(0.011)	(0.010)	(0.008)
Observations	66,225	69,827	60,019	45,316	45,568
R-squared	0.757	0.740	0.776	0.748	0.747
Panel B: Output-specific suppliers					
$\text{Post}_t \times \text{Affected Supplier}_i \times \mathbb{1}(\text{Customers}<5)_i$	-0.012	-0.012	-0.013	-0.009	-0.010
	(0.011)	(0.011)	(0.009)	(0.006)	(0.012)
$\text{Post}_t \times \text{Affected Supplier}_i \times \mathbb{1}(\text{Customers}\geq 5)_i$	0.011	0.010	0.003	0.011	0.005
	(0.014)	(0.013)	(0.014)	(0.016)	(0.013)
Observations	29,526	30,902	27,561	22,907	22,880
R-squared	0.788	0.776	0.803	0.779	0.778
Panel C: Output-specific suppliers and directly hit customers					
$\text{Post}_t \times \text{Affected Supplier}_i \times \mathbb{1}(\text{Customers}<5)_i$	-0.028	-0.033*	-0.031**	-0.035**	-0.035*
	(0.016)	(0.019)	(0.013)	(0.015)	(0.019)
$\text{Post}_t \times \text{Affected Supplier}_i \times \mathbb{1}(\text{Customers}\geq 5)_i$	0.021	0.019	0.009	0.019	0.011
	(0.019)	(0.018)	(0.016)	(0.020)	(0.017)
Observations	29,258	30,607	27,308	22,622	22,606
R-squared	0.788	0.776	0.803	0.779	0.778
Fixed Effects					
Firm	✓	✓	✓	✓	✓
Industry-Country-Year	✓				
Industry-Size Bucket-Year		✓			
Industry-Country-Size Bucket-Year			✓		
Country-Size Bucket-Linked to Affected Industry-Year				✓	
Industry-Size Bucket-Linked to Affected Industry-Year					✓

Table A.8: Effect on Suppliers' Profitability, Heterogeneity across Number of Suppliers and Product Specificity. This table presents results from Equation (3). The sample period is 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. *Affected Supplier*$_i$ is a dummy equal to one if firm i is a supplier of a directly affected firm. The dependent variable is EBIT divided by assets. The indicator variable $\mathbb{1}(\text{Customers} < 5)_i$ is equal to one if, at the time of the shock (July 2017), firm i has four or less customers in the affected industry. The indicator variable $\mathbb{1}(\text{Customers} \geq 5)_i$ is equal to one if, at the time of the shock (July 2017), firm i has five or more customers in the affected industry. The indicator variable "Linked to Affected Industry" equals one for firms that have supply chain links to industries where directly hit firms operate. In Panel A, the sample includes all suppliers. In Panel B, the sample includes suppliers with above-the-median share of R&D to sales (output-specific suppliers). In Panel C, we further restrict the sample to suppliers that provide goods and services to the directly hit firms with an above-the-median share of R&D to sales (output-specific directly hit customers). Standard errors are double clustered at the industry and country level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.

	(1) Log(1+Collateral)	(2) Pr(Default)	(3) NPL	(4) Maturity
$\text{Post}_t \times \text{Affected}_i$	-0.497	-0.004	0.006	-1.565
	(0.639)	(0.010)	(0.004)	(3.699)
Fixed Effects				
Firm	✓	✓	✓	✓
Bank-Quarter	✓	✓	✓	✓
Industry-State-Size Bucket-Quarter	✓	✓	✓	✓
Observations	93,400	134,175	166,895	107,211
R-squared	-0.020	0.600	0.048	0.554

Table A.9: Effect on Credit Terms. This table presents results from Equation (2). The period of the firm-bank matched sample for the US is 2014:Q1 to 2018:Q4. $Post_t$ is a time dummy equal to one from 2017:Q3 onward. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable is the logarithm of one plus the amount of collateral in column (1), default probability a bank assigns to a given borrower in column (2), a dummy equal to one if the loan is non-performing in column (3), and the maturity of the committed exposure in column (4). Standard errors are double clustered at the industry and bank level. *** p<0.01, ** p<0.05, * p<0.1. Source: Federal Reserve Y-14; FactSet Revere.

	(1)	(2)	(3)	(4)	(5)	(6)
	ΔEmployees			Tangible Assets/Assets		
$\text{Post}_t \times \text{Affected}_i$	0.051	0.020	0.038	0.001	0.000	0.002
	(0.060)	(0.041)	(0.031)	(0.005)	(0.003)	(0.004)
Fixed Effects						
Firm	✓	✓	✓	✓	✓	✓
Industry-Country-Size Bucket-Year	✓			✓		
Country-Size Bucket-Linked to Affected Industry-Year		✓			✓	
Industry-Size Bucket-Linked to Affected Industry-Year			✓			✓
Observations	32,060	24,603	24,796	62,304	45,582	45,885
R-squared	0.527	0.304	0.295	0.963	0.963	0.963

Table A.10: Effect on Customers' Employment and Investment. This table presents results from Equation (1). The sample period is 2014 to 2018. *Post* is a time dummy equal to one in 2017 and 2018. $Affected_i$ is a dummy equal to one if firm i is a customer of a directly affected firm. The dependent variable in columns (1)–(3) is the yearly percentage change in the number of employees. The dependent variable in columns (4)–(6) is Tangible Assets/Assets. Standard errors are double clustered at the industry and country level. *** p<0.01, ** p<0.05, * p<0.1. Source: BvD Orbis; FactSet Revere.