Stolen Secrets: The Effect of Trade Secret Theft on Corporate Innovation*

Filippo Curti† Marco Macchiavelli‡ Atanas Mihov§
Kevin Pisciotta¶

October 26, 2023

Abstract

Trade secret theft, and more broadly intellectual property (IP) theft, have resurfaced to the public attention amid the U.S.-China geopolitical conflict. In this paper, we document the detrimental effects of IP theft on innovation at the targeted firms whose trade secrets are stolen. Following the theft, targeted firms display a persistent drop in innovation outcomes, including the number of patents, patent value, and patent impact. These firms experience a decline in profitability, indicating that IP theft hurts their economic prospects. Importantly, the adverse effects of trade secret theft also spill over to the business partners of the targeted firms.

JEL classification: G30, G39, F52, O31, O32.

Keywords: IP Theft, Trade Secret Theft, Economic Espionage, Innovation, Knowledge Creation.

*The views expressed in this paper do not necessarily reflect the position of the Federal Reserve Bank of Richmond or the Federal Reserve System.

†Federal Reserve Bank of Richmond. Email: filippo.curti@rich.frb.org

‡University of Massachusetts Amherst. Email: mmacchiavelli@isenberg.umass.edu

§University of Kansas. Email: amihov@ku.edu

¶University of Kansas. Email: kpisciotta@ku.edu

1. Introduction

Corporate innovation is a vital driver of economic growth and technological advancement (Solow, 1957; Romer, 1990; Kogan et al., 2017). Companies invest substantial resources in research and development (R&D) to create proprietary technologies, products, processes, and know-how that enhance their competitiveness and contribute to societal progress. In turn, trade secrets are an integral part of a firm's operations and play a central role in safeguarding a firm's innovation and market position (Mezzanotti and Simcoe, 2023). They include a broad spectrum of confidential information that firms usually guard zealously, providing these firms with technological and competitive advantages over rivals. Trade secrets exist and depend on obscurity, different from patents or copyrights, which require public disclosure in exchange for protection. From proprietary formulas to manufacturing processes to new technologies, these undisclosed intangible assets underpin a company's uniqueness and viability. However, as the global economy becomes increasingly interconnected and nations clash for economic and geopolitical leadership, the rise of trade secret theft poses a formidable challenge to innovation-driven enterprises.[1] More importantly, the theft of trade secrets may undermine companies' abilities to generate and capitalize on novel ideas and sustain their innovation momentum.

Trade secret theft, characterized by the unauthorized acquisition of confidential business information, is executed through a wide range of activities, including employee defections and cyberattacks. Such tactics, as well as others (e.g., joint ventures with forced technological transfers), are well-exemplified in China's recent extensive effort to obtain foreign know-how (Demers, 2018; Bian and Meier, 2023). The breach of trade secrets not only exposes firms to competitive threats but may also erode the incentives for firms to invest in proprietary knowledge creation (e.g., Aghion and Howitt, 1992). While anecdotal evidence and high-profile cases highlight the adverse consequences of trade secret theft, a more systematic

[1] On November 18, 2015, William Evanina, then national counterintelligence executive of the Office of the Director of National Intelligence, estimated that economic espionage costs the U.S. economy $400 billion a year (National Bureau of Asian Research, 2017).

empirical examination of its impact on firm innovation is essential to provide researchers and policy makers with a more comprehensive understanding of the problem.

In this paper, we study the effect of trade secret theft on the innovation of targeted firms whose secrets are stolen. For ease of exposition, we use trade secret theft and intellectual property (IP) theft interchangeably, although the latter is a broader category. In a fast-paced innovation environment, the theft of trade secrets may not be an existential threat to the targeted firm. Newer technologies are continuously deployed, and the stolen IP may give the perpetrator only a short-lived, potentially one-time advantage in catching up with the target firm's technological stock of knowledge. Additionally, the theft may involve just one out of many technologies developed by the targeted firm, in which case, the adverse consequences of the theft may be limited. On the other hand, if the stolen IP is the crown jewel of the targeted firm, the consequences may be more dramatic, as the firm may lose proprietary information critical to maintaining its competitive edge and generating future innovation. In other words, the protection of these valuable assets may be paramount for the ability of the firm to innovate in the future and capture the rents from that innovation (e.g., Galasso and Schankerman, 2018).

Using novel data on incidents of trade secret theft, we document that targeted firms experience a significant decline in innovation output after the incidents. In the three years following an incident, targeted firms file fewer patents. The magnitude of this reduction is substantial — relative to a set of otherwise similar firms that do not experience IP theft, targeted firms file for 33% fewer patents per year following the incident. The economic value lost from forgone innovation is similarly non-trivial. Back-of-the-envelope estimates indicate that the average targeted firm loses around $150 million in patent value per year (during the first three years after the incident), relative to a yearly production of $480 million worth of patents for the average firm. Targeted firms' profitability ultimately declines after the theft, consistent with a deterioration of these firms' economic prospects.

We next explore the potential channels through which IP theft reduces future innova-

tion. We differentiate between two competing but not mutually exclusive channels for the reduction in innovation outcomes following trade secret theft. First, impacted firms may choose a strategy that diverts resources away from innovation-related activities, and potentially toward short-term goals related to conserving profitability. Firms have been shown to reduce R&D investment when they experience environmental, operational, and financial uncertainty, or in order to meet other short-term goals (Baber et al., 1991; Gunny, 2010; Chakravarty and Grewal, 2011). Second, firms may not significantly change their research and development, or may even increase it to "innovate their way out" of the stolen technologies and know-how. Nonetheless, the IP theft may reduce the future innovation efficiency of the company as it loses the ability to build on its proprietary information and unique aspects of its current knowledge stock. This second channel predicts that trade secret theft does not necessarily reduce the firm's innovation investment, but rather that the company loses its unique position as an innovator and experiences an associated drop in innovation quality and impact.

We find evidence consistent with the second channel. Targeted firms do not significantly change R&D spending following the trade secret theft, indicating that the channel through which IP theft reduces firm innovation is unlikely to be a resource allocation problem. Instead, we find that the fewer patents that targeted firms produce after the IP theft are less impactful as they generate fewer forward citations by subsequent patents, suggesting the quality of targeted firms' innovation also suffers. Collectively, these results are most consistent with a channel whereby the theft of technological trade secrets damages firms' abilities to monetize their innovation investment and create high quality innovation, as they lose sole possession of their trade secrets. Of note, our results are not driven by pre-trends and are robust to alternative specifications that do not rely on the logarithmic transformation of patent activity, following Cohn et al. (2022a).

Our findings so far highlight the severe consequences faced by firms unable to secure their trade secrets. However, the detrimental effects of IP theft may not stop at the targeted

firms. Rather, they may spread to the innovation activities of economically related firms as well. For example, supply-chain partners are often responsible for a significant portion of knowledge creation and innovation production that follow a focal firm's own innovation output (Cassiman and Veugelers, 2002; Chu et al., 2019; Fadeev, 2023). This occurs as firms in the supply chain share knowledge and cooperate to facilitate the production of higher-quality inputs and optimize the efficiency of the supply chain. As a result, the negative impact of trade secrets theft on firms might have broader externalities by spilling over to the innovation output of focal firms' business partners.

We indeed find negative second-round or spillover effects. Following an IP theft event, the supply-chain business partners of the targeted firms also experience a decline in innovation outcomes. The magnitude of these second-round declines is 20 to 30 percent of the (first-round) effects estimated on the targeted firms. While smaller in magnitude, since targeted firms have an average of 11 business partners, these second-round effects are quantitatively important. Back-of-the-envelope estimates suggest the average IP theft leads to an annual decline in the patent value of around $150 million for the average targeted firm and $100 million in annual total patent value for its business partners. Considering both first- and second-round losses in patents value, the average IP theft destroys a total of about $250 million in future innovation value per year.

Our paper is related to the literature on economic espionage, technological transfers, and geopolitical risk. Glitz and Meyersson (2020) show that economic espionage conducted by East Germany led to narrower industry-level productivity gaps with the West during the Cold War. In the context of the U.S.-China rivalry, Bian and Meier (2023) document how CEO myopic incentives help facilitate the systematic transfer of valuable technology from U.S. firms to Chinese firms via joint ventures. More broadly, Han et al. (2022) study technology dependence between the U.S. and China over time. Cen et al. (2022) document the industrial interdependence between the U.S. and China, focusing on the effect of Chinese industrial policy. Other studies examine the effects of U.S.-China trade wars. For example,

Flaaen et al. (2020), Benguria and Saffie (2019, 2020), and Fajgelbaum et al. (2020) examine the effects of these trade wars on U.S. imports, exports, labor markets, and the overall economy, respectively. Finally, Crosignani et al. (2023a) document the collateral damage imposed by U.S. export controls on domestic firms. We contribute to this literature by providing the first firm-level evidence of the detrimental effects of economic espionage (in the form of trade secret theft) on the innovation quantity and quality of targeted firms and their business partners.

Since a significant portion of the trade secret theft is perpetrated via cyber intrusions, we also contribute to the recent literature on cyber risk in finance. Kamiya et al. (2021), Amir et al. (2018), Scherbina and Schlusche (2023), and Curti et al. (2023) show that firms and local governments suffer significant value losses in response to the announcements of adverse cyber events. Cyber breaches appear to impact firm policies such as cash holdings, risk management, and corporate social responsibility activity (Kamiya et al., 2021; Garg, 2020; Akey et al., 2021) and generate spillover effects on firms economically linked to targeted ones (Garg, 2020; Crosignani et al., 2023b). Past research also examines the asset pricing implications of cyber risk (Jamilov et al., 2021; Florackis et al., 2023). In contrast to prior work, which is very heavily weighted towards analyzing data breaches (e.g., personal identifiable information theft), we contribute to this literature by showing that cyber vulnerabilities are also exploited to obtain trade secrets, with detrimental long-term effects on the innovation of targeted firms.

Our study also contributes new insights to the literature on corporate innovation. In particular, by showing that trade secret theft meaningfully impedes target firm innovation, we complement Cohen et al. (2019) and Mezzanotti (2021), who show that patent litigation reduces innovation activity.[2] By providing evidence on the effect of external actor actions to

[2]More broadly, we provide evidence on a new determinant of firms' innovation activity, which adds to a long list of papers documenting the effect of various firm, industry, and market characteristics on firms' innovation activities. Examples of these characteristics include private-equity ownership (Lerner et al., 2011), CEO overconfidence (Hirshleifer et al., 2012), institutional ownership (Aghion et al., 2013), financial analyst coverage (He and Tian, 2013), market conditions (Nanda and Rhodes-Kropf, 2013), corporate venture capitalists (Chemmanur et al., 2014), mergers and acquisitions (Bena and Li, 2014), firms' boundaries (Seru,

steal firm trade secrets, we also complement studies on the impact of product market competition and innovation. While prior work provides evidence that increased competition fosters innovation through increased incentives to be the first to patent inventions (Aghion et al., 2005, 2009; Levine et al., 2020), our evidence suggests competition that manifests in attacks on competitor proprietary information generates private losses in future innovation. We also contribute more broadly to the literature on institutions and innovation (e.g., Acharya and Subramanian, 2009; Acharya et al., 2013; Galasso and Luo, 2017; He and Tian, 2020), and particularly the literature examining the effects of intellectual property rights and patent protections on corporate innovation (e.g., Lerner, 2009; Galasso and Schankerman, 2015; Fang et al., 2017; Png, 2017; Galasso and Schankerman, 2018; Appel et al., 2019). Finally, our evidence of indirect adverse effects on innovation output of targeted firms' customers and suppliers are consistent with studies on innovation spillovers through the supply chain (e.g., Chu et al., 2019; Fadeev, 2023).

Our research findings are also relevant for public policy. The adverse outcomes resulting from IP theft at targeted firms highlight the critical need for public-private sector cooperation, economic incentives, and robust legal frameworks to protect firms. For example, promoting collaborations between the public and private sectors, exemplified by initiatives like the Federal Bureau of Investigation's (FBI) Office of Private Sector, can foster formulating best practices for trade secret protection and information sharing. Grants to local law enforcement agencies, like those given by the Department of Justice's (DOJ) Intellectual Property Task Force, may help to strengthen the investigation and prosecution of IP theft. Tax benefits and other incentives to firms that invest in state-of-the-art cybersecurity measures and trade secret protection can provide economic incentives to the private sector to invest in vital data defenses. Crafting legislation with precise definitions of trade secrets, delineating remedies for misappropriation, and specifying confidentiality safeguards for legal proceedings may further equip businesses with the necessary legal tools to defend their

2014), investors' attitudes toward failure (Tian and Wang, 2011), banking competition (Cornaggia et al., 2015), bank interventions (Gu et al., 2017), and external financial dependence (Acharya and Xu, 2017).

innovative assets effectively.

Finally, our results contextualize the potential benefits of effective operational risk management strategies at the firm level. Preemptive measures may involve bolstering cybersecurity frameworks, employee training on data security protocols, and implementing robust access controls to limit unauthorized data exposure. Rigorous due diligence when partnering with external parties and suppliers may similarly be essential to prevent the leakage of sensitive information. When breaches occur, firms may need swift response plans that include legal action, internal investigations, and potential collaboration with law enforcement agencies. Altogether, a proactive risk management approach may enhance a firm's resilience against trade secret theft. Nonetheless, addressing IP theft is admittedly very challenging because the openness, informality, and collaborative spirit that IP theft thrives on are also at the very core of generating technological advancements and positive knowledge and innovation spillovers. Excessive background checks, vetting, and compartmentalization of information at the firm level, while useful to prevent and detect nefarious activity, can create organizational frictions that deter innovation.

2. Background: Examples of Stolen Trade Secrets

Technologies frequently comprise multiple components of interrelated knowledge (Anton et al., 2006). Within these components, some, like codified and reverse-engineerable knowledge, are patented. Others, such as tacit knowledge, are maintained as trade secrets (Hall et al., 2014). The complementarity between different parts of knowledge makes it difficult to replicate and build on a technology without access to the knowledge that is kept secret. Conversely, developing new technologies based on a patent is significantly easier when one has access to the trade secrets associated with this patent. Firms possessing such access have a competitive edge relative to others in generating follow-on innovations (Fadeev, 2023).[3]

[3]As an example, discussions surrounding the potential waiver of intellectual property rights for COVID-19 vaccines underscored that replicating mRNA technology's success necessitates not only access to the information within patents but also access to the trade secrets and technical expertise associated with it (Price et al., 2020). The idea of complementarity between patenting and secrecy is also consistent with firm

Firms' trade secrets are increasingly under siege, as a rising tide of trade secret theft threatens not only individual businesses but also the balance of economic ecosystems on a global scale.

Trade secret theft, the clandestine act of illicitly acquiring, sharing, or utilizing another entity's confidential information, has indeed developed into a critical concern for businesses of all sizes and across many industries (e.g., National Bureau of Asian Research, 2017). The digital age has introduced not only unprecedented connectivity and accessibility, but also facilitated new avenues for criminal activity. Cyberattacks, corporate espionage, and corporate insider threats have emerged as potent tools in the arsenal of those seeking to gain an unfair advantage. The consequences of trade secret theft can be profound: targeted companies can face staggering financial losses, reputational damage, and erosion of market share, with potential spillovers to the broader network of target firms' business partners. This section highlights some illustrative cases of trade secret theft based on DOJ official releases.

A notable example of trade secret theft and its detrimental effects is the case of American Superconductor Inc. (AMSC). The company, based in the United States and specializing in energy technologies, had developed innovative software designed to enhance the energy efficiency of wind turbines. A substantial portion of its revenue was derived from selling this software to Sinovel, a prominent Chinese wind turbine manufacturer. In 2011, a disgruntled employee of AMSC, Mr. Karabasevic, who had recently been demoted but still retaining access to crucial source code, orchestrated an agreement with Sinovel. This agreement involved the unauthorized transfer of the proprietary code in exchange for a lucrative 5-year employment contract with Sinovel valued at $1 million. Once Sinovel acquired the coveted source code, they abruptly ceased their payments for the pre-existing $800 million contract with AMSC. The repercussions of this illicit act were severe: AMSC's market capitalization plummeted by $1 billion and over half of its workforce were laid off. The legal proceedings

surveys (e.g., Cohen et al., 2000), management research (e.g., Amara et al., 2008), legal research (e.g., Jorda, 2008), and case studies on IP protection in the chemical industry (e.g., Arora, 1997).

that ensued led to Sinovel's indictment in 2013 and conviction in 2018 for the theft of these trade secrets. Ultimately, the dispute culminated in a settlement, with Sinovel agreeing to pay AMSC a sum totaling $57.5 million.[4]

Another example of trade secret theft involves Micron, a leading semiconductor firm specializing in the research, development, and production of memory storage devices, notably dynamic random-access memory (DRAM) utilized in computers. Micron Memory Taiwan (MMT) was responsible for manufacturing one of Micron's DRAM chips. MMT's president, Mr. Chen, left in 2015 to join United Microelectronics Corporation (UMC), a Taiwanese semiconductor foundry. At UMC, Chen arranged a deal with Fujian Jinhua Integrated Circuits (Jinhua), a Chinese state-owned enterprise, to transfer Micron's DRAM technology to Jinhua. Chen later became Jinhua's president, managing its DRAM production. Micron sued Jinhua, which countersued for patent infringement. In October 2020, UMC pled guilty, receiving a $60 million fine and agreeing to cooperate with the U.S. government in Jinhua's prosecution.[5]

While the aforementioned examples exemplify the involvement of (former) employees in the theft of trade secrets, trade secrets are also often poached through cyber intrusions. An illustrative case involves three hackers affiliated with a Chinese internet security firm, Boyusec, who orchestrated a sophisticated "spear phishing" email campaign to illicitly breach the corporate computer systems of Trimble and Siemens.[6] In the attack on Trimble, the hackers stole commercial documents and trade secrets integral to the company's global navigation satellite system technology for mobile devices. In the attack on Siemens, the cybercriminals extracted proprietary data pertaining to the energy, technology, and transportation businesses of Siemens.[7]

[4]See *Department of Justice*: "Chinese Company Sinovel Wind Group Convicted of Theft of Trade Secrets" (January 24, 2018).

[5]See *Department of Justice*: "Taiwan Company Pleads Guilty to Trade Secret Theft in Criminal Case Involving PRC State-Owned Company" (October 28, 2020).

[6]Spear phishing attacks use social engineering tactics to lure recipients into opening attachments or clicking on links that surreptitiously install malware, thus facilitating sustained unauthorized access to the targeted computer network.

[7]See *Department of Justice*: "U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm

In another indictment, five Chinese military hackers were charged with computer hacking and economic espionage targeting Westinghouse, among other U.S. companies. During Westinghouse's construction of four power plants in China in 2010, alongside negotiations with a Chinese State Owned Enterprise (SOE) regarding various construction terms and technology transfers, the hackers illicitly acquired confidential and exclusive technical and design details pertaining to pipes, pipe supports, and pipe routing within the power plant structures. Furthermore, between 2010 and 2011, while Westinghouse was engaged in discussions about potential collaborations with the SOE, the hackers stole sensitive, strategic email communications of senior decision-makers overseeing Westinghouse's partnership with the SOE.[8]

We note, however, that despite its recent prominence, economic espionage is not a recent phenomenon, nor has it been employed by just one country. Instead, it has been widely used in history to obtain technology from countries at the technological frontier. In one instance, North American colonies resorted to extensive economic espionage to industrialize during the 18^{th} century, luring skilled workers from Great Britain (Ben-Atar, 2008). In another instance, with Operation Paperclip, the U.S. recruited, moved, and employed over 1,600 German scientists, engineers, and technicians to the United States at the end of World War II (Jacobsen, 2014). These recruited individuals possessed valuable knowledge and expertise and contributed to various fields, particularly military and aerospace technology. Last, analyses suggest the majority of Soviet military technology was the result of theft from Western countries (Andrew and Mitrokhin, 1999).

3. Hypothesis Development

There are distinct and countervailing forces that may shape the effect of trade secret theft on targeted firms' innovation activities. On the one hand, prior research argues that

for Hacking Three Corporations for Commercial Advantage" (Monday, November 27, 2017).

[8]See *Department of Justice*: "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage" (May 19, 2014).

intellectual property protection may be unnecessary in a fast-paced innovation environment (Boldrin and Levine, 2013). In fact, Lerner (2009) finds that "*the impact of patent protection-enhancing shifts on applications by residents was actually negative*" (p. 347). It is therefore possible that dynamic firms whose trade secrets are stolen respond by boosting investment in the development of the next technological advancement. Thereby the stolen technology is soon replaced by a newer and better generation, which helps the company quickly re-establish its competitive position. In that case, IP theft could either have no effect or even temporarily boost future innovation by the targeted firm if, for instance, the firm desires to expedite new technology development as a way to make its "stolen secrets" obsolete.

On the other hand, trade secret theft can profoundly erode a company's innovation output via two main channels, in line with Schumpeterian growth theories (e.g., Aghion and Howitt, 1992; Aghion et al., 2015).[9] The first channel operates through a reduction in research and development spending following an IP theft event. One potential reason for this reduction is resource diversion, both in terms of financial investment directed towards legal action and operational risk management, as well as the reallocation of human capital away from productive innovation efforts. Another potential reason is that when a company's trade secrets are stolen, R&D investment uncertainty increases. Specifically, there's an increased risk that the return on investment made into research and development could significantly decrease – e.g., because the firm's innovations can be more easily replicated. As a result, businesses might become reluctant to invest significant additional resources into in-process innovations or new projects and breakthrough technologies, as the required return needs to be much higher to compensate for the increased risk. Either of these – resource diversion or higher innovation project risk – could lead to a slowdown in R&D efforts and a decrease in innovation output.

The second channel instead operates through "a significant negative shock" (by the trade secret theft) to the competitive standing of the targeted firm's stock of knowledge and

[9]While these growth theories make predictions that account for general equilibrium effects, our prediction is purely a partial equilibrium one that only considers innovation incentives at the individual firm level.

innovative assets in place, which are hard to replace or redevelop. Stolen trade secrets can be replicated or exploited by competitors, eroding the uniqueness and impact of a firm's stock of in-process innovation. Specifically, following theft, proprietary trade secrets, which may be crucial for the development of future innovation, are no longer privately held but rather revealed to key competitors thus diminishing the targeted firm's competitive advantage for producing innovation (particularly over the short and medium term). Consistent with this idea, Galasso and Schankerman (2018) argue "the ability of a firm to innovate in the future ... will depend on the firm's current stock of patents" (p.65), and thus also its cumulative body of proprietary information and intellectual property. Another reason is that when trade secrets are stolen, perpetrators may also make it hard for the targeted firm to even access the stolen (knowledge) assets, leading to a loss of expertise that underpins high-quality innovation efforts. As a result of either competitive degradation of in-process innovation or loss of access to stolen assets, the company loses its unique position as an innovator, leading to a reduced ability to produce high quality innovation.

Given the tension in the two-sided predictions above, we state our main hypothesis in the null form as follows:

Hypothesis 1: *Trade secret theft does not affect the innovation output of the targeted firm.*

4. Empirical Design and Sample Construction

4.1. Empirical Design

We study the effect of trade secret theft on target firm innovation using the following difference-in-differences (DiD) specification:

$$y_{it} = \beta Post\text{-}IP\ Theft_{it} + \delta X + \mu_i + \mu_{kt} + \varepsilon_{it}, \tag{1}$$

where y_{it} measures the innovation outcomes of interest — patent quantity and quality — of firm i during year t. We measure innovation quantity as (the natural logarithm of one

plus) the number of patents filed, or alternatively as (the natural logarithm of one plus) the market value of firm i's patents (based on the stock market reaction to the patent grants). We measure innovation quality and impact as (the natural logarithm of one plus) the average number of forward patent citations per patent filing. To address concerns raised by Cohn et al. (2022b) with "log one plus" regressions, particularly when used with count-like variables such as the number of patent filings, we show in Section 6.3 that our conclusions are unchanged when we estimate Poisson regressions as well as unlogged regressions of scaled and unscaled patent quantity.

Post-IP Theft$_{it}$ is an indicator variable equal to one during the years after an IP theft incident targeted at firm i is noticed by the firm. Following the design of Heese et al. (2022), we restrict our focus to the six years surrounding the notice date ($-3 \leq j \leq 3$). X is a set of lagged controls, including the natural logarithm of the firm's market value of equity and age (years available on Compustat), liquidity (cash-to-assets ratio), book-to-market ratio, and a "high-tech" indicator equal to one for technology stocks (Loughran and Ritter, 2004). We also include firm and industry-year fixed effects, denoted by μ_i and μ_{kt}, respectively. To futher limit the influence of differences in firms' life cycles across our comparison groups, in more restrictive specifications, we include firm and industry-year-age decile fixed effects. Standard errors are clustered at the firm level.

Although we present results using the DiD model of Eq. (1) with a full panel of firm-fiscal years, we also rely on characteristics-based matching that compares the innovation of treated firms with the innovation of a more restricted set of control firms of similar size, age, and industry to treated firms during the same period. We focus our characteristics-based matching on identifying control firms of similar size and age because those characteristics have been shown to be important determinants of firms' innovation output and strategy (e.g., Huergo and Jaumandreu, 2004; Bernstein, 2015). To construct the characteristics-matched sample, for each treated firm we require control firms to be in the same Fama French (FF) 12 industry and have never been a target of trade secret theft, then take the ten closest

peer firms in terms of age, and then the five closest remaining firms in terms of assets as of the year of the trade secret theft event. Hereafter, we refer to this sample constructed by characteristics-based matching as the "matched sample."

Even though the fixed effects structure in our DiD model and our characteristics-based matching method reduce the heterogeneity across treatment and control groups, biased estimates may still arise if treated firms systematically differ from control firms leading up to treatment. For instance, treated firms may already be on a downward innovation trajectory prior to the trade secret theft. In this case, the estimated effect would be clouded by pre-trends. Alternatively, it may be the case that innovation dynamics follow an inverted U-shaped dynamic, and the trade secret theft occurs at peak innovation and thus any observed decline in firm innovation after the attacks may again be spurious. We address these concerns in Section 5.1 by showing that when using either our baseline sample or our matched sample, we observe no systematic differences in innovation patterns between treated and control firms leading up to the trade secret theft incidents.

Although firms targeted by IP theft are not a random sample — rather, they are targeted because they possess a specific technology of interest — there are two economic reasons for the similar pre-trends between treated and control firms (conditional on the controls in our models). One reason is that, given the specific and targeted technological needs of the attackers, it is likely that among two similar firms (A and B) with similar innovation trends, firm A possess a technology that the attacker wants to acquire while firm B produces a different technology that the attacker is currently not targeting. As a result, firm A gets targeted and has its trade secret stolen, but not firm B. Alternatively, within the technologies that an attacker wants to obtain, they may cast a wide net, targeting several companies developing these technologies. Among this set, the actual company that is successfully targeted and whose trade secrets are stolen may be considered quasi-random.. Therefore, it is possible that the attacker targets two similar firms (C and D) in the same industry and with similar innovation trends, but can only infiltrate firm C. In this case, the researcher

would observe a case of trade secret theft for firm C, but not the attempted infiltration of firm D, which is likely to serve as a control unit.

It is important to note that our estimates in Eq. (1) are likely a lower bound of the true effect of trade secret theft on corporate innovation. As some trade secret theft events are not reported or prosecuted and therefore not included in the treatment group, we may have some truly treated firms erroneously classified as control firms. Such mis-classification leads to attenuation bias and results in our coefficients likely underestimating the true causal effect of IP theft on firms' future innovation.

4.2. Sample Construction

We combine five sources of data in our analysis. Data on trade secret theft come from the U.S. Department of Justice (DOJ) and Zywave (formerly Advisen), a leading provider of operational risk incidents. We hand-collect cases of trade secret theft from the DOJ website (https://www.justice.gov/news) by searching the following keywords: IP theft; trade secret; economic espionage. We also filter press releases by the topics of intellectual property and national security. We obtain a total of 72 unique theft incidents from DOJ indictments, excluding multiple records pertaining to the same case. For instance, if there are 2 press releases (indictment and conviction) for the same case, we only include it once. We collect the press release data of the indictment, the start and end dates of the crime committed, and the names of the target companies that have their trade secrets stolen.

Although a few cases involve hospitals, government agencies, or universities as targets, most cases involve publicly- and privately-traded companies. In two cases, the names of the target companies are redacted and cannot be found through news searches. We are able to match a total of 40 target companies on Compustat. We retain only the first event for each target company, which reduces the sample to 31 cases. Most cases target U.S. companies in the agriculture, energy, electronics, and semiconductor sectors.

We supplement these data we collect from the DOJ with data from Zywave, a company that collects operational risk incidents from public sources such as media, legal, or public

filings and records. These data cover cyberattacks (e.g., data breaches and ransomware attacks), as well as incidents involving the loss of personal information and trade secrets, either executed by cyber intrusion, exfiltrated by an employee, or lost by mistake. The dataset includes incident and announcement dates, the name of the targeted company, the type of incident, and a description of the incident. We focus on incidents involving the corporate loss of digital assets (CLDA). Within the CLDA subsample, we manually read the description of each incident from Zywave and from public sources (LexisNexis and internet searches) and retain only those involving trade secret theft. Out of 107 CLDA events from 2000 to 2020 (after collecting only the first event for each target company), we retain 27 CLDA events related to the theft of trade secrets.[10] We thus have a total of 58 unique trade secret theft events between the two samples. While many events may go unreported or undetected, this sample is the most comprehensive set of IP theft events we are aware of.

We then construct a firm-fiscal year panel from Compustat between 2000 and 2020. The vast majority of our baseline sample of 110,775 firm-fiscal years is comprised of firms never subject to trade secret theft. There are a total of 11,387 firms in the sample (58 of which are subject to IP theft during our sample period). As we discuss further below, we address the imbalance in our sample between treated and control firms by conducting analysis using a matched sample of treated and control firms, where, again, control firms are matched to treated firms on industry, size, and age.

Our measures of firm innovation output (patent quantity and quality) are based on patenting activity. Our data on patenting come from Kogan et al. (2017) and contain information on patent filing and issuance dates for granted patents, CRSP PERMNO identifiers of patent assignees, forward patent citations, and implied stock market values of the patents. This data set consists of all U.S. patents granted during the period 1926-–2020 (3,053,011) linked to U.S. public firms, excluding patents assigned to multiple companies. We comple-

[10]We ensure no overlap between the DOJ and Zywave samples. As part of this step of going from 107 CLDA events to 27, we exclude six events due to overlap between the two samples. Most of the trade secret theft cases from Zywave that do not overlap with the DOJ sample involve indictments filed in non-U.S. jurisdictions, or other cases that do not culminate in a DOJ indictment.

ment our innovation output measures with company financial information from Compustat, including R&D and SG&A expenditures, profitability, firm size, age, cash holdings, and book-to-market ratios.

Finally, we collect data from Compustat Segments on supplier-customer relationships between firms. These data list names of a firm's main customers, which are mostly other firms but can also be government agencies. Regulation SFAS No. 131 requires publicly traded firms to report the identity of any customer representing more than 10% of their total sales. We also utilize data from Cohen and Frazzini (2008), Cen et al. (2017) and Mihov and Naranjo (2017), which links suppliers and customers (using name matching and manual inspection) for U.S. publicly traded firms during our sample period.

We report summary statistics for our sample in Table 1. Firms that experience IP theft ("Treated") tend to be larger, older, and have higher growth options (lower book-to-market ratio) than firms that do not experience theft ("Control"), as shown in Panel A. Panel B shows that even though the average ratio of R&D expenditures to assets is similar between treated and control firms, treated firms produce many more patents and create more patent value than control firms. These differences are intuitive, since IP theft is a purposeful decision by actors to acquire valuable technologies. We mitigate the influence of this selection by using restrictive sets of fixed effects, controlling for predictors of innovation outcomes, and utilizing a characteristics-based matching approach that selects control firms in the same industry as treated firms and closest in size and age at the time of the events.

[Insert Tables 1 and 2 here]

Table 2 reports the time series and industry distribution of our treatment events. From Panel A, most of the trade secret theft occurs after 2006. The years with the highest number of incidents are 2013, 2009 and 2016. Panel B of Table 2 shows that most of the events occur in Business Equipment and Other industries, followed by Manufacturing, Chemicals, Durables, and Money. Energy, Health, and Shops experience a small number of incidents

as well. This distribution overlaps with some of the highly targeted sectors in economic espionage.

5. Regression Results

5.1. The Effect of Trade Secret Theft on Innovation

We begin our empirical analysis by estimating the average effect of trade secret theft on innovation output, measured by the natural logarithm of one plus the number of patents a company files in a given year, *Ln(1+#Patents)*. Table 3, Panel A presents the results. Column (1) estimates Eq. (1) with firm and industry-year fixed effects using the full sample of firms; Column (2) uses firm and more granular industry-year-age decile fixed effects to account for differences in innovation patterns depending on the age of the firm; and Column (3) adds additional (time-varying) controls. Finally, Column (4) uses the matched sample with firm and matched pair-year fixed effects, in addition to the controls used in Column (3).

Across the four specifications, the coefficient of interest (*Post-IP Theft)* is negative and stable, indicating a statistically and economically significant decline in firms' patent filings following trade secret theft. Based on our most restrictive specification in Column (4), the magnitude of the coefficient suggests a 33% relative annual decline in the number of patents filed by treated firms compared with otherwise similar control firms.[11] The magnitude of this effect is somewhat smaller but on the same order of magnitude as compared with a company losing a patent right, which, according to Galasso and Schankerman (2018), leads to a 50% reduction in firms' patent activities over the subsequent five years.

[Insert Table 3 here]

As previously discussed in Section 4.1, the observed differences in patent activity following

[11] The 33% decline is obtained by taking the exponential of the -0.397 estimate in Column (4) and subtracting 1.

trade secret theft could be driven by systematic differences between treated and control units prior to the IP theft event. For instance, theft may occur at the natural peak of firms' innovation cycles. We address such potential bias by including industry-year-age decile fixed effects in our regressions in Table 3, as these indicators restrict comparisons among treated and control firms of similar age in the same industry and year. Additionally, our matched sample holds constant the event year and requires treated and control firms to share similar characteristics. To more directly address the possibility that treated firms are at a different stage in their innovation cycles compared with control firms, we check for pre-trends in the relative innovation activity of treated firms preceding the event of the theft.

Figure 1 shows a coefficient plot of a dynamic version of Eq. (1). Specifically, we plot the event-year specific coefficients of relative innovation activity (i.e., the difference in innovation output between treated and control firms) surrounding trade secret theft events, setting the trade secret theft year as our base year. If treated firms are at peak innovation when breached, we should expect significantly negative coefficients prior to the trade secret theft. If instead, the theft event follows an extraordinary amount of innovation, we would observe significantly positive coefficients prior to the trade secret theft.

[Insert Figure 1 here]

However, as shown in Figure 1, the estimated coefficients prior to the IP theft are not statistically significant, and thus show no evidence of pre-trends. This suggests that IP theft is potentially directed at specific technologies and has some degree of randomness regarding which specific technology the attackers manage to obtain among the set of targeted technologies. Indeed, it does not appear that successful IP theft incidents systematically occur among firms at peak innovation or that recently experienced extraordinary levels of innovation relative to control firms. Overall, we interpret the results in this section as consistent with trade secret theft leading to a reduction in future innovation, rejecting the null hypothesis (Hypothesis 1) that IP theft does not affect the innovation output of targeted

firms.

We conclude this section by providing a back of the envelope calculation on the economic value of innovation lost after the occurrence of trade secret theft. Estimating the value of stolen trade secrets is complicated by the lack of publicly available information on the exact technology stolen. We consequently take a more general approach and estimate the loss in the value of future innovations, which is separate from the value of the stolen trade secret itself. To do this, we use a measure of the market value of patents based on stock market reactions to patent grants estimated by Kogan et al. (2017). We construct an analogical new variable to *Ln(1+#Patents)*, *Ln(1+Patent Value)*, by substituting the number of patents with their market value. Table 3, Panel B reports the results from estimating Eq. (1) using the market value of firms' patents as the dependent variable.

Across all specifications in the, the coefficient of interest, *Post-IP Theft*, is significantly negative and stable across specifications, indicating that trade secret theft reduces the economic value of firms' innovations. The detrimental effects of IP theft on innovation quality are also economically significant. From Column (4), the average theft event reduces the dollar value of patent grants by 31% per year. Because the average firm-year in the regression sample produces about $470 million in innovation value per year, a rough approximation suggests this estimate translates into a relative reduction of $150 million per year.

5.2. Evidence on the Economic Mechanism

The results in the previous section indicate that trade secret theft degrades target firms' abilities to produce patented innovation. Section 3 outlines the two main channels that could generate this effect. First, the targeted may decrease their investment in innovation. This could occur, for example, because targeted firms shift resources away from innovative activities. Second, the targeted company may lose its unique position as an innovator, not because it invests significantly less in innovation, but because it is no longer able to sustain its high quality innovation output — i.e., the trade secret theft degrades the competitive

viability of the targeted firm's stock of knowledge and its capacity to produce future impactful innovation.

We differentiate between these two competing, although not mutually exclusive, channels through two sets of tests. Our first set of tests examines firms' R&D and sales, general, and administrative (SG&A) expenditures following IP theft incidents. We follow a large literature that relies on R&D expenditures as a measure of corporate investment in innovation (see related discussions in Atanassov (2013); Faleye et al. (2014); Dambra et al. (2023)), noting that R&D expenditures help capture the initiation of innovation activity. SG&A, while noisier, captures another useful aspect of innovation investment, namely spending on top inventors and skilled worker training (Eisfeldt and Papanikolaou, 2013). Exploring the behavior of R&D and SG&A following IP theft events can inform us whether investment in innovation changes significantly in the aftermath of such events. Table 4 reports results from regression specifications similar to Eq. (1), where R&D expenditures is the dependent variable in Panel A and SG&A expenditures is the dependent variable in Panel B. Both are scaled by firms' lagged assets.

[Insert Table 4 here]

Across all specifications in the two panels, the coefficients on *Post-IP Theft* are insignificant at conventional levels. This result suggests that trade secret theft does not significantly affect either measure of innovation investment. Consequently, although innovation output significantly decreases following IP theft events, as shown in Section 5.1, innovation investment does not. These results are consistent with the notion that the declines in innovation quantity are not driven by the reallocation of resources away from innovative investment.

Our second set of tests examines the effect of trade secret theft on targeted firms' innovation quality. To measure innovation quality we focus on the impact of produced patents on future innovation captured by the forward citations of a patent (Moretti, 2021; Akcigit et al., 2022; Aghion et al., 2023). Specifically, we use (the natural logarithm of one

plus) the average number of forward citations per patent filed by the firm during year t, *Ln(1+#Cites/Patents)*.

Table 5 reports the results from estimating Eq. (1) using our measure of innovation quality. Across all specifications in the table, the coefficient of interest, *Post-IP Theft*, is significantly negative and stable across specifications, indicating that trade secret theft reduces the quality of firms' innovations.

[Insert Table 5 here]

Overall, these results have important implications as they suggest that the declines in innovation quantity are not driven by the reallocation of resources. Rather, subsequent to the theft of trade secrets, the target firm's capacity to convert innovation investment into high-quality and high-impact output appears to decline, consistent with the idea that trade secrets often represent specialized, industry-specific knowledge that is hard to replace. Thus, remedial policies in response to IP theft threats aimed at allowing access to financing are unlikely to be successful.

6. Additional Analyses and Robustness

6.1. Corporate Profitability After Trade Secret Theft

Because of the critical role of firm-level innovation for firms' prospects and viability (e.g., Kogan et al., 2017), our previous results imply that the theft of trade secrets should generate meaningful threats to the targeted firms' economic prospects. We examine this question next by studying the effect of trade secret theft on firm profitability as well as its likelihood of becoming unprofitable.

[Insert Table 6 here]

Table 6 presents results from regressions similar to Eq. (1) with both full and matched

samples, using measures of firm profitability as dependent variables. In Panel A, we use return on assets measured by firms' net income scaled by lagged assets (*ROA*). In Panel B, we use an indicator variable for whether firms report negative earnings (*Earnings Loss*) in a given year.

The results across the four specifications in each panel show that trade secret theft reduces firms' profitability and increases the likelihood that firms experience earnings losses during the three years after the theft. These effects are economically significant. The coefficients in Column (4) of Panels A and B suggest that an IP theft incident reduces ROA by 0.023, or roughly 0.13 of its standard deviation, and increases the probability of an earnings loss by 6.7 percentage points, or 35% relative to the mean probability of 19.4 percent, respectively. These results introduce an additional layer of evidence that corroborates our previous findings. By hindering the firm's ability to monetize existing IP and leverage existing IP into future ideas and products, IP theft reduces the economic prospects of targeted firms.

6.2. Innovation Spillovers Along the Supply Chain

Our results so far have underscored the adverse consequences on the innovation outcomes of firms fallen victim to trade secret theft. The adverse consequences of IP theft, however, may extend beyond the immediately affected firms. Instead, they can spread to the innovation activities of economically interconnected entities along firms' supply chains. Indeed, supply-chain partners significantly contribute to the creation of knowledge and innovation following a focal firm's innovations (Cassiman and Veugelers, 2002; Manso, 2011; Chu et al., 2019; Fadeev, 2023). This stems from technological complementarity, knowledge sharing and collaborative efforts within the supply chain, aimed at enhancing product quality and optimizing operational efficiency. Consequently, the deleterious effects of trade secrets theft on firms can generate broader externalities, impacting the innovation output of the focal firms' business associates.

In this section, we test whether the negative innovation effect of IP theft propagates

through the target companies' supply chains and generates negative spillovers (i.e., second-round effects). To estimate these potential spillover effects, we employ a variant of Eq. (1) where the main regressor, Post-IP Theft, equals one for the customers and suppliers (called business partners) of the targeted firms following the IP theft event. Table 7 displays the results.

[Insert Table 7 here]

The dependent variable in Panel A is the number of patents that a business partner of a targeted firm files for. Across all specifications, the effect of IP theft at a targeted firm on its business partners' innovation quantity is negative and significant. The detrimental effect of IP theft on firm innovation indeed propagates through the supply chain. The magnitude of this second-round effect ranges from -0.066 to -0.093, relative to a coefficient of about -0.380 for the first-round effect on the firms directly targeted by IP theft (shown in Table 3). Specifically, the second-round effect is about 20 percent of the first-round effect. As economic intuition would suggest, this negative spillover effect is smaller in magnitude relative to the first-round effect experienced by the targeted firms.

Panel B of Table 7 consistently shows a significant drop in patent value at target firms' business partners. (In this case, the second-round effects are at about one-third of the magnitude of the first-round effects.) Even though the second-round effect is smaller in magnitude than the first-round one, because the average targeted firm has 11 business partners, the aggregate scale of the second-round effect is economically significant. Specifically, the patent value lost due to the first-round effects is about $150 million per year for the average IP theft event, while the additional loss due to second-round effects is an economically large $100 million.[12] Our results are consistent with the literature that establishes innovation spillovers via supply chain relations, and suggest that the implications of IP theft are not just felt by

[12]To get to the back-of-the-envelope second-round estimate of $100 million in total patent value lost for the average IP theft event, we multiply the implied percentage decline from the coefficient estimate of -0.117 in Column (4) (-11.04%) by the average number of business partners of the average targeted firm (11) and the average annual patent value of the firms in that regression sample ($80 million).

the targeted firm, but also by the broader set of business partners.

6.3. Re-specification of Regression Model

The distribution of the number of patent applications is well known to be skewed to the right (e.g., Dambra et al., 2023). To address this skewness and retain firm-years with zero patent applications, our main specifications based on Eq. (1) use the log of one plus the number of patent applications as the dependent variable. However, ordinary least squares (OLS) coefficients may be biased, inconsistent, and potentially uninterpretable when there is a large proportion of zero observations (Cohn et al., 2022b). Hence, we also consider two sets of alternative specifications presented in Table 8.

[Insert Table 8 about here]

In our first set of alternative specifications in Columns (1) and (2), we use a different estimator, a fixed effects Poisson regression, to estimate Eq. (1), using the unscaled number of patents as the dependent variables. In our second set of alternative specifications in Columns (3) and (4), we use OLS regressions but instead of the log-transformed number of patents, we use the number of patents scaled by lagged assets.

Across all four specifications, patent activity declines following trade secret theft. The estimated effect remains statistically significant, indicating our results are robust to alternative models and measures of patent activity are unlikely to be a byproduct of the concerns with patent regressions using log transformations on count-based dependent variables with large proportions of zero values.

7. Conclusion

Trade secret theft is an important tool in economic espionage that provides unfair competitive advantages to the perpetrators, while being potentially detrimental to the targeted

individuals and businesses. Trade secret theft has gained a lot of prominence over the last two decades among a number of highly publicized cases, and against the backdrop of intensifying geopolitical tensions and economic rivalry among nations. In this paper, we use a novel dataset to study the effects of trade secret theft on the innovation output of firms whose trade secrets are stolen.

We find that targeted firms experience a decline in innovation output and quality following trade secret theft, relative to similar but unaffected firms. Specifically, trade secret theft events reduce the number of patents, the market value of patents, and the number of patent forward citations in the three years after the theft events. The result is not driven by pre-existing trends in the relative innovation activity of treated and control firms. Targeted firms do not display a decline in innovation investment (i.e., R&D and SG&A expenditures) following the IP theft events, indicating that the channel through which IP theft reduces firm innovation is unlikely to be a resource diversion problem. We argue the target firms' ability and efficiency in converting innovation investment into high-quality and high-impact output decline due to the loss of proprietary information (e.g., key competitors learning and using information about target firms' proprietary technologies). Trade secret theft has broader implications for the prospects of targeted firms, as their future profitability is negatively affected. We also importantly document that the negative effects of IP theft on innovation output do not stop at the targeted firms. Rather, they also spill over along the supply chain to negatively impact the innovation output of the targeted firms' business partners.

Our findings contextualize the detrimental effects of trade secret theft on corporate innovation and have important implications. Strengthening operational risk management and implementing robust legal safeguards are necessary to protect intellectual property and ensuring sustained innovation momentum within organizations. Furthermore, policymakers, industry associations, and international bodies must collaborate to establish comprehensive frameworks that deter and address trade secret theft, while being mindful that excessive controls and compartmentalization may deter future knowledge creation.

References

Acharya, V., and Z. Xu. 2017. Financial dependence and innovation: The case of public versus private firms. *Journal of Financial Economics* 124:223–243.

Acharya, V. V., R. P. Baghai, and K. V. Subramanian. 2013. Wrongful discharge laws and innovation. *Review of Financial Studies* 27:301–346.

Acharya, V. V., and K. V. Subramanian. 2009. Bankruptcy codes and innovation. *Review of Financial Studies* 22:4949–4988.

Aghion, P., U. Akcigit, and P. Howitt. 2015. The Schumpeterian growth paradigm. *Annual Reviews of Economics* 7:557–575.

Aghion, P., A. Bergeaud, and J. V. Reenen. 2023. The impact of regulation on innovation. *American Economic Review, forthcoming*.

Aghion, P., N. Bloom, R. Blundell, R. Griffith, and P. Howitt. 2005. Competition and innovation: An inverted-U relationship. *Quarterly Journal of Economics* 120:701–728.

Aghion, P., R. Blundell, R. Griffith, P. Howitt, and S. Prantl. 2009. The effects of entry on incumbent innovation and productivity. *Review of Economics and Statistics* 91:20–32.

Aghion, P., and P. Howitt. 1992. A model of growth through creative destruction. *Econometrica* 60:323–351.

Aghion, P., J. Van Reenen, and L. Zingales. 2013. Innovation and institutional ownership. *American Economic Review* 103:277–304.

Akcigit, U., D. Hanley, and S. Stantcheva. 2022. Optimal taxation and R&D policies. *Econometrica* 90:645–684.

Akey, P., S. Lewellen, I. Liskovich, and C. Schiller. 2021. Hacking corporate reputations. *Rotman School of Management Working Paper No. 3143740*.

Amara, N., R. Landry, and N. Traoré. 2008. Managing the protection of innovations in knowledge-intensive business services. *Research Policy* 37:1530–1547.

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

Andrew, C., and V. Mitrokhin. 1999. *The Sword And The Shield: The Mitrokhin Archive And The Secret History Of The KGB*. Basic Books.

Anton, J. J., H. Greene, and D. A. Yao. 2006. Policy implications of weak patent rights. *Innovation Policy and the Economy* 6:1–26.

Appel, I., J. Farre-Mensa, and E. Simintzi. 2019. Patent trolls and startup employment. *Journal of Financial Economics* 133:708–725.

Arora, A. 1997. Patents, licensing, and market structure in the chemical industry. *Research Policy* 26:391–403.

Atanassov, J. 2013. Do hostile takeovers stifle innovation? Evidence from antitakeover legislation and corporate patenting. *Journal of Finance* 68:1097–1131.

Baber, W. R., P. M. Fairfield, and J. A. Haggard. 1991. The effect of concern about reported income on discretionary spending decisions: The case of research and development. *The Accounting Review* 66:818–829.

Ben-Atar, D. S. 2008. *Trade secrets: Intellectual piracy and the origins of American industrial power*. Yale University Press.

Bena, J., and K. Li. 2014. Corporate innovations and mergers and acquisitions. *Journal of Finance* 69:1923–1960.

Benguria, F., and F. Saffie. 2019. Dissecting the impact of the 2018-2019 Trade War on U.S. exports. *Working paper, Available at SSRN 3505413*.

Benguria, F., and F. Saffie. 2020. The impact of the 2018-2019 Trade War on U.S. local labor markets. *Working paper, Available at SSRN 3542362*.

Bernstein, S. 2015. Does going public affect innovation. *Journal of Finance* 70:1365–1403.

Bian, B., and J.-M. Meier. 2023. Did Western CEO incentives contribute to China's technological rise? *Working paper, Available at SSRN 3949536*.

Boldrin, M., and D. K. Levine. 2013. The case against patents. *Journal of Economic Perspectives* 27:3–22.

Cassiman, B., and R. Veugelers. 2002. R&D cooperation and spillovers: Some empirical evidence from Belgium. *American Economic Review* 92:1169–1184.

Cen, L., E. L. Maydew, L. Zhang, and L. Zuo. 2017. Customer–supplier relationships and corporate tax avoidance. *Journal of Financial Economics* 123:377–394.

Cen, X., V. Fos, and W. Jiang. 2022. A race to lead: How Chinese government interventions shape U.S.-China production competition. *Working paper, Available at SSRN 3564494*.

Chakravarty, A., and R. Grewal. 2011. The stock market in the driver's seat! Implications for R&D and marketing. *Management Science* 57:1594–1609.

Chemmanur, T. J., E. Loutskina, and X. Tian. 2014. Corporate venture capital, value creation, and innovation. *Review of Financial Studies* 27:2434–2473.

Chu, Y., X. Tian, and W. Wang. 2019. Corporate innovation along the supply chain. *Management Science* 65:2445–2466.

Cohen, L., and A. Frazzini. 2008. Economic links and predictable returns. *Journal of Finance* 63:1977–2011.

Cohen, L., U. G. Gurun, and S. D. Kominers. 2019. Patent trolls: Evidence from targeted firms. *Management Science* 65:5461–5486.

Cohen, W. M., R. R. Nelson, and J. P. Walsh. 2000. Protecting their intellectual assets: Appropriability conditions and why U.S. manufacturing firms patent (or not). *Working Paper 7552, National Bureau of Economic Research* .

Cohn, J. B., Z. Liu, and M. I. Wardlaw. 2022a. Count (and count-like) data in finance. *Journal of Financial Economics* 146:529–551.

Cohn, J. B., Z. Liu, and M. I. Wardlaw. 2022b. Count (and count-like) data in finance. *Journal of Financial Economics* 146:529–551.

Cornaggia, J., Y. Mao, X. Tian, and B. Wolfe. 2015. Does banking competition affect innovation? *Journal of Financial Economics* 115:189–209.

Crosignani, M., L. Han, M. Macchiavelli, and A. F. Silva. 2023a. Geopolitical Risk and Decoupling: Evidence from U.S. Export Controls. *Working paper, Available at SSRN 4563485*.

Crosignani, M., M. Macchiavelli, and A. F. Silva. 2023b. Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics* 147:432–448.

Curti, F., I. Ivanov, M. Macchiavelli, and T. Zimmermann. 2023. City Hall Has Been Hacked! The Financial Costs of Lax Cybersecurity. *Working paper, Available at SSRN 4465071*.

Dambra, M., A. Mihov, and L. Sanz. 2023. Disclosure Processing Costs and Corporate Innovation. *Working Paper, Available at SSRN: 4417411*.

Demers, J. 2018. China's non-traditional espionage against the United States: The threat and potential policy responses. Statement Before the Senate Committee on the Judiciary, Washington, D.C. (December 12, 2018). Department of Justice.

Eisfeldt, A. L., and D. Papanikolaou. 2013. Organization capital and the cross-section of expected returns. *Journal of Finance* 68:1365–1406.

Fadeev, E. 2023. Creative construction: Knowledge sharing and cooperation between firms. *Working Paper*.

Fajgelbaum, P. D., P. K. Goldberg, P. J. Kennedy, and A. K. Khandelwal. 2020. The return to protectionism. *Quarterly Journal of Economics* 135:1–55.

Faleye, O., T. Kovacs, and A. Venkateswaran. 2014. Do better-connected CEOs innovate more? *Journal of Financial and Quantitative Analysis* 49:1201–1225.

Fang, L. H., J. Lerner, and C. Wu. 2017. Intellectual property rights protection, ownership, and innovation: Evidence from China. *Review of Financial Studies* 30:2446–2477.

Flaaen, A., A. Hortaçsu, and F. Tintelnot. 2020. The production relocation and price effects of US trade policy: the case of washing machines. *American Economic Review* 110:2103–27.

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

Galasso, A., and H. Luo. 2017. Tort reform and innovation. *Journal of Law and Economics* 60:385–412.

Galasso, A., and M. Schankerman. 2015. Patents and cumulative innovation: Causal evidence from the courts. *Quarterly Journal of Economics* 130:317–369.

Galasso, A., and M. Schankerman. 2018. Patent rights, innovation, and firm exit. *RAND Journal of Economics* 49:64–86.

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

Glitz, A., and E. Meyersson. 2020. Industrial espionage and productivity. *American Economic Review* 110:1055–1103.

Gu, Y., C. X. Mao, and X. Tian. 2017. Banks' interventions and firms' innovation: Evidence from debt covenant violations. *Journal of Law and Economics* 60:637–671.

Gunny, K. A. 2010. The relation between earnings management using real activities manipulation and future performance: Evidence from meeting earnings benchmarks. *Contemporary Accounting Research* 27:855–888.

Hall, B., C. Helmers, M. Rogers, and V. Sena. 2014. The Choice between Formal and Informal Intellectual Property: A Review. *Journal of Economic Literature* 52:375–423.

Han, P., W. Jiang, and D. Mei. 2022. Mapping U.S.-China technology decoupling: Policies, innovation, and firm performance. *Working Paper, Available at SSRN: 3779452* .

He, J., and X. Tian. 2020. Institutions and innovation. *Annual Review of Financial Economics* 12:377–398.

He, J. J., and X. Tian. 2013. The dark side of analyst coverage: The case of innovation. *Journal of Financial Economics* 109:856–878.

Heese, J., G. Pérez-Cavazos, and C. D. Peter. 2022. When the local newspaper leaves town: The effects of local newspaper closures on corporate misconduct. *Journal of Financial Economics* 145:445–463.

Hirshleifer, D., A. Low, and S. H. Teoh. 2012. Are overconfident CEOs better innovators? *Journal of Finance* 67:1457–1498.

Huergo, E., and J. Jaumandreu. 2004. Firms' age, process innovation and productivity growth. *International Journal of Industrial Organization* 22:541–559.

Jacobsen, A. 2014. *Operation Paperclip: The Secret Intelligence Program that Brought Nazi Scientists to America*. Little, Brown and Company.

Jamilov, R., H. Rey, and A. Tahoun. 2021. The anatomy of cyber risk. *Working Paper, Available at SSRN: 3886659*.

Jorda, K. F. 2008. Patent and trade secret complementariness: An unsuspected synergy. *Washburn Law Journal* 48:1–32.

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

Kogan, L., D. Papanikolaou, A. Seru, and N. Stoffman. 2017. Technological innovation, resource allocation, and growth. *Quarterly Journal of Economics* 132:665–712.

Lerner, J. 2009. The empirical impact of intellectual property rights on innovation: Puzzles and clues. *American Economic Review* 99:343–348.

Lerner, J., M. Sorensen, and P. Strömberg. 2011. Private equity and long-run investment: The case of innovation. *Journal of Finance* 66:445–477.

Levine, R., C. Lin, L. Wei, and W. Xie. 2020. Competition laws and corporate innovation. *Working Paper 27253, National Bureau of Economic Research*.

Loughran, T., and J. Ritter. 2004. Why Has IPO Underpricing Changed over Time? *Financial Management* 33:5–37.

Manso, G. 2011. Motivating innovation. *Journal of Finance* 66:1823–1860.

Mezzanotti, F. 2021. Roadblock to innovation: The role of patent litigation in corporate R&D. *Management Science* 67:7362–7390.

Mezzanotti, F., and T. Simcoe. 2023. Innovation and appropriability: Revisiting the role of intellectual property. *Working Paper 31428, National Bureau of Economic Research*.

Mihov, A., and A. Naranjo. 2017. Customer-base concentration and the transmission of idiosyncratic volatility along the vertical chain. *Journal of Empirical Finance* 40:73–100.

Moretti, E. 2021. The effect of high-tech clusters on the productivity of top inventors. *American Economic Review* 111:3328–75.

Nanda, R., and M. Rhodes-Kropf. 2013. Investment cycles and startup innovation. *Journal of Financial Economics* 110:403–418.

National Bureau of Asian Research. 2017. The theft of American intellectual property: Reassessments of the challenge and United States policy.

Png, I. P. 2017. Law and innovation: Evidence from state trade secrets laws. *Review of Economics and statistics* 99:167–179.

Price, W. N., A. K. Rai, and T. Minssen. 2020. Knowledge transfer for large-scale vaccine manufacturing. *Science* 369:912–914.

Romer, P. M. 1990. Endogenous technological change. *Journal of Political Economy* 98:71–102.

Scherbina, A., and B. Schlusche. 2023. The effect of malicious cyber activity on the U.S. corporate sector. *Working Paper, Available at SSRN 4400066*.

Seru, A. 2014. Firm boundaries matter: Evidence from conglomerates and R&D activity. *Journal of Financial Economics* 111:381–405.

Solow, R. M. 1957. Technical change and the aggregate production function. *Review of Economics and Statistics* 39:312–320.

Tian, X., and T. Y. Wang. 2011. Tolerance for failure and corporate innovation. *Review of Financial Studies* 27:211–255.

Figure 1: Innovation Dynamics around IP Theft Events

This figure plots coefficients from firm-fiscal year level DiD regressions estimating the relation between IP theft events and corporate innovation. The outcome variable, *Ln(1+#Patents)*, is the natural logarithm of one plus the number of patents filed by firm i during fiscal year t. We interact our main treatment indicator variable (*IP Theft*), which is equal to one during the three years beginning the year of an IP theft event, with indicators for the three event years preceding the event year and the three event years following the IP theft event. Each point on the line represents one of these interaction coefficients. The coefficient on the event year 0 interaction is normalized to zero. Each regression is estimated using our characteristics-based matched sample and includes firm and match-by-year fixed effects. The vertical line at event year 0 marks the transition from the pre-incident period to the post-incident period. The vertical bars denote 95% confidence intervals.

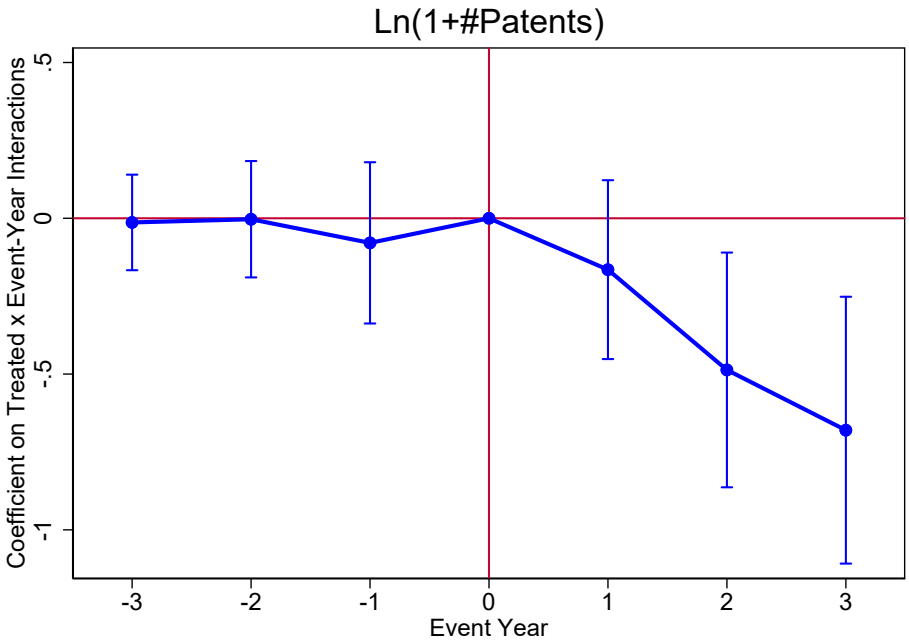

Figure 2: Innovation Dynamics of Connected firms Surrounding IP Theft Events
This figure plots coefficients from firm-fiscal year level DiD regressions estimating the spillover effects of IP theft events on connected firms' corporate innovation. The outcome variable, *Ln(1+#Patents)*, is the natural logarithm of one plus the number of patents filed by firm i during fiscal year t. We interact our spillover treatment indicator variable (*IP Theft*), which is equal to one during the three years beginning the year of an IP theft event for the customer or supplier of firm i, with indicators for the three event years preceding the event year and the three event years following the IP theft event. Each point on the line represents one of these interaction coefficients. The coefficient on the event year 0 interaction, representing the average effect among control firms, is normalized to zero. Each regression uses our characteristics-based matched sample amd includes firm and match-by-year fixed effects. The vertical line at event year 0 marks the transition from the pre-incident period to the post-incident period. The vertical bars denote 95% confidence intervals.

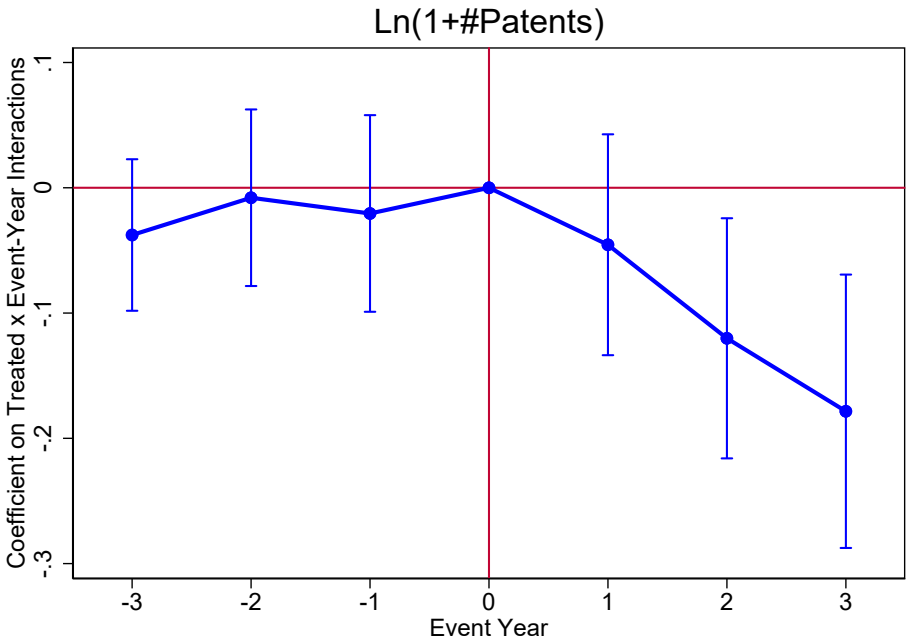

Table 1: Summary Statistics

This table reports mean, median, standard deviation, and sample size summary statistics for our explanatory and outcome variables. Panel A summarizes firm characteristics at the firm-fiscal year level for our full sample. Panel B reproduces Panel A for our characteristics-based matched sample. Panel C describes our innovation, expenditures, and profitability outcomes variables for the full sample. Panel D reproduces Panel C our the matched sample. The sample of firm-fiscal years begins in 2000 and ends in 2020. Variables are defined in Appendix A.

Panel A: Firm Characteristics

	Control Firms				Treated Firms			
Variable	Mean	Median	SD	N	Mean	Median	SD	N
Assets ($ Mil)	6,686.90	644.60	23,221.26	110,444	36,571.87	14,012.00	51,349.68	331
Market Cap ($ Mil)	3,843.27	454.94	10,504.37	110,444	23,725.01	13,483.31	24,727.90	331
Firm Age	18.40	14.00	14.84	110,444	31.20	22.00	21.50	331
Book-to-Market	0.70	0.54	0.99	110,444	0.47	0.38	0.72	331
Cash/Assets	0.20	0.10	0.24	110,444	0.18	0.12	0.17	331
High-tech	0.08	0.00	0.27	110,444	0.09	0.00	0.28	331

Panel B: Matched-Sample Firm Characteristics

	Matched-Control Firms				Treated Firms			
Variable	Mean	Median	SD	N	Mean	Median	SD	N
Assets ($ Mil)	15,924.18	4,630.85	32,086.50	10,599	35,834.12	13,936.50	50,719.50	326
Market Cap ($ Mil)	10,884.92	3,791.82	16,787.11	10,599	23,390.07	12,953.91	24,459.05	326
Firm Age	29.38	23.00	19.66	10,599	31.38	22.00	21.56	326
Book-to-Market	0.55	0.43	0.68	10,599	0.47	0.37	0.73	326
Cash/Assets	0.14	0.09	0.16	10,599	0.18	0.12	0.17	326
High-tech	0.14	0.00	0.35	10,599	0.08	0.00	0.27	326

Panel C: Outcome Variables

	Control Firms				Treated Firms			
Variable	Mean	Median	SD	N	Mean	Median	SD	N
# Patents	3.90	0.00	15.37	110,444	37.72	17.00	41.64	331
R&D/Assets	0.06	0.00	0.17	110,024	0.05	0.03	0.08	330
SG&A/Assets	0.26	0.13	0.51	110,024	0.17	0.15	0.15	330
Patent Value	37.57	0.00	172.51	110,444	488.40	248.05	503.89	331
# Citations/Patents	1.14	0.00	3.65	110,444	2.21	0.34	4.05	331
ROA	−0.08	0.02	0.66	109,979	0.03	0.05	0.17	330
Loss Indicator	0.34	0.00	0.48	110,444	0.23	0.00	0.42	331
Patents/Assets	3.67	0.00	10.77	110,024	8.58	1.28	13.48	330
Patents/Expenditures	0.01	0.00	0.02	84,970	0.03	0.01	0.03	272

Panel D: Matched Sample Outcome Variables

	Matched-Control Firms				Treated Firms			
Variable	Mean	Median	SD	N	Mean	Median	SD	N
# Patents	15.36	0.00	30.63	10,796	37.05	17.00	41.52	331
R&D/Assets	0.03	0.00	0.07	10,786	0.05	0.03	0.08	330
SG&A/Assets	0.17	0.13	0.23	10,786	0.16	0.15	0.13	330
Patent Value	174.29	0.00	358.45	10,796	485.22	248.05	503.17	331
# Citations/Patents	1.98	0.00	4.36	10,796	2.06	0.32	3.85	331
ROA	0.04	0.04	0.18	10,784	0.04	0.05	0.14	330
Loss Indicator	0.19	0.00	0.39	10,796	0.22	0.00	0.42	331
Patents/Assets	4.84	0.00	11.26	10,786	8.21	1.21	13.10	330
Patents/Expenditures	0.02	0.00	0.03	8,923	0.02	0.01	0.03	269

Table 2: Temporal and Industrial Distribution of Trade Secret Theft Events

This table reports the number of trade secret theft incidents for the 58 treated firms in our primary regression sample. Panel A reports the number of incidents in each fiscal year. Panel B reports the number of incidents in each Fama-French 12-Industry.

Panel A: Distribution by Fiscal Year

Fiscal Year	Incidents
2000	1
2001	1
2005	2
2006	1
2007	4
2008	3
2009	6
2010	2
2011	6
2012	2
2013	11
2014	4
2015	6
2016	4
2018	4
2019	1
Total	58

Panel B: Distribution by Industry Sector

Industry Sector	Incidents
Business Equipment	15
Chemicals	5
Durables	4
Energy	3
Health	2
Manufacturing	8
Money	4
Non-Durables	1
Other	14
Shops	2
Total	58

Table 3: Trade Secret Theft and Corporate Innovation Output

This table reports results from OLS regressions examining the relation between IP theft and firm innovation. Columns (1)–(3) employ the standard difference-in-differences model of Equation (1), while Column (4) uses the characteristics-based matched sample (i.e., "*Matched Sample*"). The matched sample includes, for each treated firm, the five closest peer firms in terms of age and size in the FF12 industry of the treated firm. The dependent variable in Panel A, *Ln(1+# Patents)*, is the natural logarithm of one plus the number of patents filed by firm i during fiscal year t. The dependent variable in Panel B, *Ln(1+Patent Value)*, is the natural logarithm of one plus the total stock market value of patents filed by firm i during fiscal year t. We include the full time series for firms that do not experience an IP theft event and event years (−3,+3) for firms that experience an IP theft event. *Post-IP Theft* is an indicator variable equal to one during the three years beginning the year firm i notices their first IP theft event. For DOJ indictments, we use the start year of the incident to estimate when the firm notices the theft. *Industry-Year-Age FE* represents industry-by-year-by annually-sorted age decile fixed effects. The regression sample begins in 2000 and ends in 2020. Control variables are defined in Appendix A. Standard errors are clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A: Number of Patents

				Matched Sample
	(1) Ln(1+# Patents)	(2) Ln(1+# Patents)	(3) Ln(1+# Patents)	(4) Ln(1+# Patents)
Post-IP Theft	−0.397***	−0.373***	−0.374***	−0.397***
	(−3.07)	(−2.87)	(−2.89)	(−3.05)
Ln(Market Cap)			0.051***	0.105***
			(11.53)	(4.75)
Ln(Firm Age)			0.133***	0.912
			(4.70)	(1.50)
Book-to-Market			0.010***	0.065***
			(4.04)	(3.52)
Cash/Assets			0.083***	0.183
			(3.14)	(0.88)
High-tech			−0.363	−0.189
			(−1.03)	(−0.80)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.808	0.815	0.809	0.881
Observations	143,043	143,014	110,775	11,127

Panel B: Patent Value

				Matched Sample
	(1) Ln(1+ Patent Value)	(2) Ln(1+ Patent Value)	(3) Ln(1+ Patent Value)	(4) Ln(1+ Patent Value)
Post-IP Theft	−0.465**	−0.412**	−0.413**	−0.373**
	(−2.52)	(−2.25)	(−2.26)	(−1.97)
Ln(Market Cap)			0.070***	0.188***
			(10.73)	(5.86)
Ln(Firm Age)			0.252***	1.848*
			(5.60)	(1.81)
Book-to-Market			0.007**	0.093***
			(2.09)	(3.28)
Cash/Assets			0.115***	0.272
			(3.02)	(0.89)
High-tech			−0.366	−0.057
			(−0.80)	(−0.15)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.806	0.814	0.808	0.865
Observations	143,043	143,014	110,775	11,127

Table 4: Innovation Investment

This table reports results from OLS regressions examining the relation between IP theft and firms' innovation-related expenditures. Columns (1)–(3) employ the standard difference-in-differences model of Equation (1), while Column (4) uses the characteristics-based matched sample (i.e., "*Matched Sample*). The matched sample includes, for each treated firm, the five closest peer firms in terms of age and size in the FF12 industry of the treated firm. The dependent variable in Panel A, *R&D/Assets*, is the ratio of research and development expenditures over lagged total assets. The dependent variable in Panel B, *SG&A/Assets*, is the ratio of sales, general, and administrative expenditures over lagged total assets. We include the full time series for firms that do not experience an IP theft event and event years (−3,+3) for firms that experience an IP theft event. *Post-IP Theft* is an indicator variable equal to one during the three years beginning the year firm i notices their first IP theft event. For DOJ indictments, we use the start year of the incident to estimate when the firm notices the theft. *Industry-Year-Age FE* represents industry-by-year-by annually-sorted age decile fixed effects. The regression sample begins in 2000 and ends in 2020. Control variables are defined in Appendix A. Standard errors are clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A: R&D

				Matched Sample
	(1) R&D/ Assets	(2) R&D/ Assets	(3) R&D/ Assets	(4) R&D/ Assets
Post-IP Theft	−0.002	−0.003	−0.003	−0.007
	(−0.47)	(−0.54)	(−0.57)	(−1.35)
Ln(Market Cap)			0.003***	−0.002
			(3.73)	(−0.80)
Ln(Firm Age)			−0.027***	−0.073*
			(−4.87)	(−1.75)
Book-to-Market			−0.002***	0.000
			(−5.42)	(0.36)
Cash/Assets			0.055***	0.017
			(8.79)	(1.22)
High-tech			0.005	−0.005
			(0.37)	(−0.81)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.715	0.731	0.733	0.714
Observations	110,746	110,720	110,242	11,113

Panel B: SG&A

				Matched Sample
	(1) SG&A/ Assets	(2) SG&A/ Assets	(3) SG&A/ Assets	(4) SG&A/ Assets
Post-IP Theft	0.015**	0.016	0.017	0.010
	(1.97)	(1.41)	(1.37)	(1.11)
Ln(Market Cap)			−0.002	−0.008*
			(−0.70)	(−1.95)
Ln(Firm Age)			−0.231***	−0.331***
			(−8.28)	(−3.01)
Book-to-Market			−0.012***	−0.006**
			(−7.26)	(−2.26)
Cash/Assets			0.138***	0.033
			(4.83)	(0.97)
High-tech			−0.002	−0.015
			(−0.05)	(−0.57)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.472	0.492	0.499	0.502
Observations	110,699	110,673	110,242	11,113

Table 5: Innovation Quality

This table reports results from OLS regressions examining the relation between IP theft and the quality of targeted firms' innovation. Columns (1)–(3) employ the standard difference-in-differences model of Equation (1), while Column (4) uses the characteristics-based matched sample (i.e., "*Matched Sample*). The matched sample includes, for each treated firm, the five closest peer firms in terms of age and size in the FF12 industry of the treated firm. The dependent variable, *Ln(1+ Cites/Patents)*, is the natural logarithm of one plus the number of citations received per patent filed by firm i during fiscal year t. We include the full time series for firms that do not experience an IP theft event and event years (−3,+3) for firms that experience an IP theft event. *Post-IP Theft* is an indicator variable equal to one during the three years beginning the year firm i notices their first IP theft event. For DOJ indictments, we use the start year of the incident to estimate when the firm notices the theft. *Industry-Year-Age FE* represents industry-by-year-by annually-sorted age decile fixed effects. The regression sample begins in 2000 and ends in 2020. Control variables are defined in Appendix A. Standard errors are clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

				Matched Sample
	(1) Ln(1+ #Cites/Patents)	(2) Ln(1+ #Cites/Patents)	(3) Ln(1+ #Cites/Patents)	(4) Ln(1+ #Cites/Patents)
Post-IP Theft	−0.162***	−0.133***	−0.135***	−0.111*
	(−3.73)	(−2.80)	(−2.83)	(−1.92)
Ln(Market Cap)			0.016***	0.032
			(3.29)	(1.42)
Ln(Firm Age)			0.180***	−0.657
			(5.38)	(−0.91)
Book-to-Market			−0.001	0.023
			(−0.24)	(1.44)
Cash/Assets			0.131***	−0.018
			(4.22)	(−0.11)
High-tech			−0.101	−0.222
			(−0.42)	(−0.85)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.560	0.567	0.555	0.691
Observations	143,043	143,014	110,775	11,127

Table 6: Profitability and Earnings Loss

This table reports results from OLS regressions examining the relation between IP theft and firm profitability. Columns (1)–(3) employ the standard difference-in-differences model of Equation (1), while Column (4) uses the characteristics-based matched sample (i.e., "*Matched Sample*). The matched sample includes, for each treated firm, the five closest peer firms in terms of age and size in the FF12 industry of the treated firm. The dependent variable in Panel A, *ROA*, is the ratio of net income and lagged total assets. The dependent variable in Panel B, *Earnings Loss*, is an indicator variable equal to one if the firms' net income during year t is less than zero. We include the full time series for firms that do not experience an IP theft event and event years (−3,+3) for firms that experience an IP theft event. *Post-IP Theft* is an indicator variable equal to one during the three years beginning the year firm i notices their first IP theft event. For DOJ indictments, we use the start year of the incident to estimate when the firm notices the theft. *Industry-Year-Age FE* represents industry-by-year-by annually-sorted age decile fixed effects. The regression sample begins in 2000 and ends in 2020. Control variables are defined in Appendix A. Standard errors are clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A: Return on Assets

				Matched Sample
	(1) ROA	(2) ROA	(3) ROA	(4) ROA
Post-IP Theft	−0.049***	−0.059***	−0.060***	−0.023**
	(−3.32)	(−2.89)	(−2.90)	(−2.05)
Ln(Market Cap)			0.038***	0.041***
			(8.06)	(7.68)
Ln(Firm Age)			0.295***	0.172
			(5.81)	(1.18)
Book-to-Market			0.011***	0.000
			(2.97)	(0.09)
Cash/Assets			−0.177***	0.174**
			(−4.04)	(2.34)
High-tech			0.096	−0.023
			(1.23)	(−1.06)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.335	0.350	0.356	0.275
Observations	110,636	110,612	110,193	11,112

Panel B: Earnings Loss

				Matched Sample
	(1) Loss Indicator	(2) Loss Indicator	(3) Loss Indicator	(4) Loss Indicator
Post-IP Theft	0.082**	0.091**	0.094**	0.067*
	(2.16)	(2.35)	(2.55)	(1.69)
Ln(Market Cap)			−0.130***	−0.135***
			(−51.31)	(−14.33)
Ln(Firm Age)			−0.018	−0.120
			(−1.10)	(−0.43)
Book-to-Market			0.022***	0.007
			(10.47)	(0.87)
Cash/Assets			−0.109***	−0.212***
			(−7.23)	(−3.09)
High-tech			0.113*	0.214***
			(1.90)	(3.86)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.472	0.475	0.519	0.412
Observations	111,049	111,026	110,597	11,123

Table 7: Spillovers

This table reports results from OLS regressions examining the spillover effects of IP theft events on the innovation activity of business partners of the firms that are the targets of the theft. We identify business partners as firms that are either customers or suppliers, during any of the three years leading up to as IP Theft event, of the 58 firms in our primary sample that are targets of IP theft. Columns (1)–(3) of Panels A, B, and C employ the standard difference-in-differences model of Equation (1). Column (4) of Panels A, B, and C use the characteristics-based matched sample (i.e., "*Matched Sample*). The matched sample includes, for each treated business partner, the five closest peer firms in terms of age and size in the industry of the treated business partner. The dependent variable in Panel A, *Ln(1+# Patent)*, is the natural logarithm of one plus the number of patents filed by firm i during fiscal year t. The dependent variable in Panel B, *Ln(1+Patent Value)*, is the natural logarithm of one plus the total stock market value of patents filed by firm i during fiscal year t. We include the full time series for control firms (i.e., firms that neither experience an IP theft event nor are customers or suppliers of firms that experience an IP theft event) and event years (−3,+3) for firms that are customers or suppliers of firms that experience an IP theft event. *Post-IP Theft* is an indicator variable equal to one during the three years beginning the year the customer or supplier of firm i notices their first IP theft event. For DOJ indictments, we use the start year of the incident to estimate when the customer or supplier firm notices the theft. *Industry-Year-Age FE* represents industry-by-year-by annually-sorted age decile fixed effects. The regression sample begins in 2000 and ends in 2020. Control variables are defined in Appendix A. Standard errors are clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A: Number of Patents

				Matched Sample
	(1) Ln(1+# Patents)	(2) Ln(1+# Patents)	(3) Ln(1+# Patents)	(4) Ln(1+# Patents)
Post-IP Theft	−0.086***	−0.093***	−0.090***	−0.066**
	(−3.24)	(−3.51)	(−3.40)	(−2.40)
Ln(Assets)			0.084***	0.126***
			(9.18)	(7.36)
Ln(Firm Age)			0.046**	−0.016
			(2.10)	(−0.39)
Book-to-Market			−0.019***	−0.030***
			(−3.63)	(−2.95)
Cash/Assets			0.151***	0.166***
			(4.68)	(2.94)
High-Tech			0.165	−0.020
			(1.07)	(−0.13)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.806	0.814	0.809	0.804
Observations	153,437	153,416	121,111	48,628

Panel B: Patent Value

				Matched Sample
	(1) Ln(1+ Patent Value)	(2) Ln(1+ Patent Value)	(3) Ln(1+ Patent Value)	(4) Ln(1+ Patent Value)
Post-IP Theft	−0.140***	−0.146***	−0.145***	−0.117***
	(−3.13)	(−3.23)	(−3.20)	(−2.65)
Ln(Market Cap)			0.077***	0.117***
			(9.62)	(8.26)
Ln(Firm Age)			0.272***	−0.137
			(4.98)	(−0.57)
Book-to-Market			0.007*	0.001
			(1.67)	(0.17)
Cash/Assets			0.085*	−0.004
			(1.96)	(−0.05)
High-tech			−0.088	0.023
			(−0.34)	(0.23)
Firm FE	Yes	Yes	Yes	Yes
Industry–Year FE	Yes	No	No	No
Industry–Year–Age FE	No	Yes	Yes	No
Matched Pair–Year FE	No	No	No	Yes
Adj. R-squared	0.807	0.815	0.809	0.827
Observations	149,456	149,428	117,143	42,057

Table 8: Alternative Patent Measures and Poisson Regressions

This table reports results from Poisson and OLS regressions examining the relation between IP theft and firm innovation. Columns (1) and (2) use Poisson regressions, while Columns (3) and (4) use OLS regressions. The dependent variable in Columns (1) and (2) is the number of patents filed by firm i during year t. The dependent variable in Columns (3) and (4) is the number of patents filed by firm i during year t scaled by lagged total firm assets Columns (1) and (3) use the full sample, while Columns (2) and (4) use the characteristics-based matched sample. The matched sample includes, for each treated firm, the five closest peer firms in terms of age and size in the FF12 industry of the treated firm. We include the full time series for firms that do not experience an IP theft event and event years (−3,+3) for firms that experience an IP theft event. *Post-IP Theft* is an indicator variable equal to one during the three years beginning the year firm i notices their first IP theft event. For DOJ indictments, we use the start year of the incident to estimate when the firm notices the theft. *Industry-Year-Age FE* represents industry-by-year-by annually-sorted age decile fixed effects. The regression sample begins in 2000 and ends in 2020. Control variables are defined in Appendix A. Standard errors are clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

		Matched Sample		Matched Sample
	(1) Unscaled Patents	(2) Unscaled Patents	(3) Patents/ Assets	(4) Patents/ Assets
Post-IP Theft	−0.148**	−0.260***	−1.551*	−1.859**
	(−2.50)	(−4.02)	(−1.72)	(−2.13)
Ln(Market Cap)	0.413***	0.341***	0.225***	0.261
	(7.41)	(8.57)	(3.81)	(1.36)
Ln(Firm Age)	−0.682	−3.646	0.278	−0.992
	(−1.35)	(−1.09)	(0.72)	(−0.22)
Book-to-Market	0.317***	0.072	−0.097***	0.087
	(2.89)	(1.03)	(−3.43)	(1.05)
Cash/Assets	0.168	0.597	3.653***	6.102**
	(0.79)	(1.53)	(8.24)	(2.51)
High-tech	−1.047*	−0.144	1.368	0.466
	(−1.84)	(−0.19)	(0.89)	(0.16)
Estimator	Poisson	Poisson	OLS	OLS
Firm FE	Yes	Yes	Yes	Yes
Industry–Year–Age FE	Yes	No	Yes	No
Matched Pair–Year FE	No	Yes	No	Yes
Adj. R-squared	0.594	0.737	0.594	0.737
Observations	39,311	5,541	110,242	11,113

Appendix

A. Variable Definitions

This table reports definitions and sources for all variables used in the paper.

Variable Name	Description
# Patents	The number of patents filed by firm i between the fiscal year end of year t and the fiscal end of year $t+1$. *Source:* USPTO, Kogan et al. (2017).
# Cites/Patents	The number of citations received by patents filed by firm i between the end of fiscal year t and the end of fiscal year $t+1$, scaled by the number of patents filed by firm i during that period. *Source:* Kogan et al. (2017).
Patent Value	The cumulative stock market value, in $ million, of patents filed by firm i between the fiscal year end of year t and the fiscal end of year $t+1$. *Source:* USPTO, Kogan et al. (2017).
Assets	The total assets (at) of firm i, in $ million, as of the fiscal year end date in year t. *Source:* Compustat.
Book-to-Market	The book value of firm i's assets, minus the book value of firm i's liabilities, scaled by the market capitalization of firm i's equity as the fiscal year end date in year t. *Source:* Compustat.
Cash/Assets	The amount of firm i's cash and cash equivalents, scaled by the firm's assets. *Source:* Compustat.
Firm Age	The number of years firm i is available on Compustat as of the fiscal year end date in year t. *Source:* Compustat.
High-tech	An indicator variable equal to one if firm i's SIC code is one of the 33 SIC codes identified by Loughran and Ritter (2004) as being associated with "Tech stocks." *Source:* CRSP.
Earnings Loss	An indicator variable equal to one if firm i's net income is less than zero during fiscal year t. *Source:* Compustat.
Market Cap	The market capitalization of firm i's equity as the fiscal year end date in year t. *Source:* Compustat.
Patents/Assets	The number of patents filed by firm i between the fiscal year end of year t and the fiscal end of year $t+1$, scaled by the firm's assets (at) as of the end of the fiscal year end date in year $t-1$. *Source:* USPTO, Kogan et al. (2017), Compustat.
Post-IP Theft	An indicator variable equal to one during the three fiscal years beginning the year firm i notices an IP theft incident targeted at the firm. For DOJ incidents, we identify the notice date as the start date of the attack noted in the DOJ indictment. *Source:* DOJ and Zywave.
R&D/Assets	The R&D expenditures (xrd) of firm i during fiscal year t scaled by firm i's total assets (at) as the end of the fiscal year $t-1$. If R&D is missing, we set it to zero. *Source:* Compustat.
ROA	The net income (ni) of firm i during fiscal year t, scaled by the firm's total assets (at) as of the end of fiscal year $t-1$. *Source:* Compustat.
SG&A/Assets	The SG&A expenditures (xrd) of firm i during fiscal year t scaled by firm i's total assets (at) as the end of the fiscal year $t-1$. If SG&A is missing, we set it to zero. *Source:* Compustat.