The Value of Trade Secrets: Evidence from Economic Espionage*

December 2024

Alexander Michaelides
Imperial College London
and CEPR

Andreas Milidonis
University of Cyprus

Vitaliy Ryabinin
Indiana University Northwest

Yupana Wiwattanakantang
National University of Singapore
and EGCI

*We thank seminar participants at the Hong Kong Polytechnic University (Hong Kong), and the National Central University (Taiwan) for useful comments. All remaining errors are our own. Michaelides' contact address is Department of Finance, Imperial College Business School, South Kensington Campus, London, SW72AZ, UK; a.michaelides@imperial.ac.uk. Milidonis' contact address is Department of Accounting & Finance, School of Economics & Management, University of Cyprus, P.O. Box 20537, CY-1678 Nicosia, Cyprus; andreas.milidonis@ucy.ac.cy. Ryabinin's contact address is Indiana University Northwest, 3400 Broadway, Dunes Medical/Professional Building 1127, Gary, IN 46408; viryab@iu.edu. Wiwattanakantang's contact address is Department of Finance, NUS Business School, National University of Singapore, 15 Kent Ridge Dr, Mocthar Riady Building, Singapore 119245; yupana@nus.edu.sg.

Abstract

The Value of Trade Secrets: Evidence from Economic Espionage

We estimate a lower bound of trade secrets' aggregate value, a key component of intangible capital. We hand-collect criminal cases involving trade secret theft filed under the Economic Espionage Act of 1996. Victim firms are notably larger than an average S&P 500 constituent. The value of trade secrets is substantial, with the average market value loss corresponding to $1.6–2.1 billion. Aggregating across all events between 1996 and 2019, the total loss exceeds $190 billion. For at least three years after the theft, victim firms acquire other firms, potentially to replenish their intangible capital.

Keywords: Value of Trade Secrets, Intangible Capital, Economic Espionage.

JEL Classification: G14, G15, G24.

1 Introduction

Intangible capital contributes significantly to company stock market valuations[1] and economic growth.[2] While patents are a critical component of intangible capital (e.g., Kogan et al. (2017)), trade secrets are also a key component of intangible value, but have not received significant research attention. Anecdotal evidence does suggest that trade secrets are valuable and amenable to theft by competitors with industrial espionage arising in industries ranging from agriculture to high technology.[3] Although the exact economic value of trade secrets held by U.S. firms is unknown, the U.S. Chamber of Commerce estimates that they may account for as much as 80% of the firm's information portfolio (United States Chamber of Commerce (2013)). A U.S. Senate expert testimony estimates the 2014 value between 1% and 3% of GDP ($150 billion to $450 billion).[4] To protect trade secrets, the U.S. government enacted the Economic Espionage Act of 1996 (EEA) to criminalize trade secret thefts, and therefore involve federal authorities like the Federal Bureau of Investigation (FBI).[5]

We contribute to the literature by offering empirical evidence on the economic significance of trade secrets. In our empirical analysis we use the criminal cases filed by the U.S. Department of Justice (DoJ) prosecuted under the EEA. We carefully track the information transmission process related to publicly traded, victim firms whose trade secrets have been stolen. Using event studies we document a significant loss in market value around the initial announcement of a trade secret theft. We

[1] See for example, Eisfeldt et al. (2021), Crouzet and Eberly (2023b), Ewens et al. (2023).

[2] Endogenous growth (Romer (1990)) relies on the power of ideas and intangible capital (Haskel and Westlake (2018)) to sustain economic growth (Aghion and Howitt (1992), Howitt (2000)).

[3] Hvistendahl (2021) describes industrial espionage in Iowa farms targeting genetically modified seeds, while *The Financial Times* describes a suspected case of trade secret theft for California tech startups; September 25, 2024; https://www.ft.com/content/d94a5467-ebf9-4992-af13-3e71061707a4.

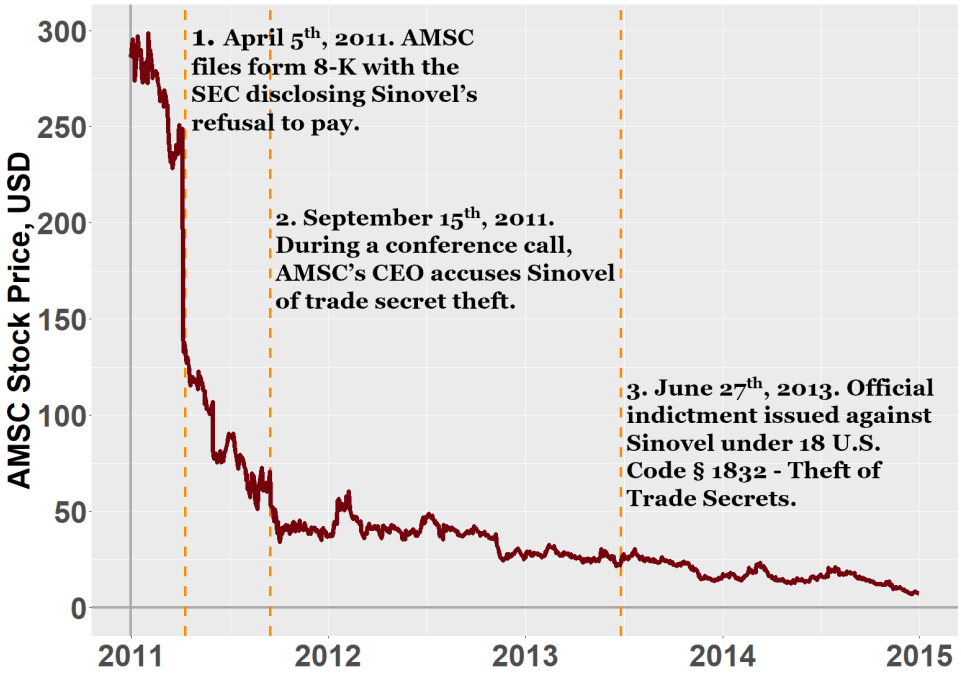
[4] Testimony on "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"; US Senate Committee on the Judiciary (2014), Passman et al. (2014), U.S. Government Publishing Office, May 13, 2014 records; https://www.govinfo.gov/content/pkg/CHRG-113shrg96009/html/CHRG-113shrg96009.htm.

[5] In 2013, the value of trade secrets received further attention through the 2013 Presidential Strategy that emphasized the significant economic damage caused by intellectual property thefts to the competitiveness of American industries (Office of the Intellectual Property Enforcement Coordinator (2013)).

estimate a lower bound of trade secrets held by large firms with an aggregate value of approximately $190 billion between 1996 and 2019.

Figure 1: **AMSC Stock Price and Trade Secret Theft Timeline**

This figure presents AMSC's stock price around key trade secret theft events and court filings (dashed vertical lines).



To illustrate our approach to value trade secrets, in Figure 1 we show the stock market response to a trade secret theft experienced by American Superconductor (Ticker: AMSC). AMSC is a clean energy technology developer and manufacturer, specializing in both production and transmission of electricity. On March 31, 2011, Sinovel, AMSC's largest client responsible for over 70% of its revenue, refused to pay and accept shipments, and stopped licensing the software from AMSC. On April 5, 2011, AMSC filed an 8-K notice alerting shareholders.[6] A drastic price decrease of over 80% immediately followed. On September 14, 2011, AMSC filed a lawsuit

[6]See https://ir.amsc.com/node/11761/html.

in China against Sinovel for trade secret theft.[7] On a conference call the next day AMSC's CEO accused Sinovel of trade secret theft and the stock price further declined over the following two years. On June 27, 2013, the DoJ issued an official indictment against Sinovel stating also that the case was investigated by the FBI, and the AMSC share price declined further. Around five years later, Sinovel was convicted for stealing AMSC trade secrets.[8] The DoJ press release on July 6, 2018, revealed that the AMSC software was stolen by an ex-employee for the benefit of Sinovel on March 7th, 2011.

This example illustrates the events that can be used to estimate the value of trade secrets. At the same time, the example reveals the challenges in identifying the exact event date when trade secret loss is reflected in the stock price. The largest market reaction might indicate the firm losing a major client and/or trade secrets among other unobservable reasons. To avoid this confounding information problem, we focus on cases that involve the official trade secret theft announcement by the DoJ; and the cases have not been featured by the media. In other words, we focus on cases where indictments have a very high chance of being the first ever public mention, and estimate the stock market reaction to these filings.

We construct our sample starting in October 1996, when the EEA was implemented. Until June 2021, the DoJ had pursued 253 criminal prosecutions under U.S. Code §1831 (Economic Espionage) and U.S. Code §1832 (Theft of Trade Secrets) of the EEA (Fang and Li (2021)). This sample includes private firms, international firms and firms listed in the U.S. exchanges. We focus on firms listed in U.S. stock markets. To mitigate any information leakage prior to the DoJ charges, we parse through news articles related to each trade secret theft, and we err on the side of caution by removing cases where the trade secret theft was likely known to the public before the DOJ charge.

Our sample consists of 72 cases over the period 1996 to 2019 and covers companies

[7]See https://ir.amsc.com/news-releases/news-release-details/amsc-filing-criminal-and-civil-complaints-against-sinovel.

[8]See https://www.justice.gov/opa/pr/court-imposes-maximum-fine-sinovel-wind-group-theft-trade-secrets.

spanning 20 different industries. In our sample, victim firms are notably larger than an average S&P 500 constituent. The average market capitalization of victim firms at the time of theft is about $120 billion (in 2020 dollars) compared to the S&P500 companies' average of $64 billion in 2020 (year end). Using a linear probability model on the universe of US firms, we document that firms associated with trade secret thefts rely more heavily on intangibles, are large and have low cash flow. These results are robust to controlling for different intangibility measures, both based on accounting data and patent citations (Peters and Taylor (2017), Kogan et al. (2017)).

Our main contribution is an estimate of the market value of trade secrets. We rely on a short-horizon event study with the DoJ announcements of trade secret misappropriation serving as the event days. A part of our sample is sealed cases (i.e. those restricted from public view), allowing us to provide some evidence consistent with the leakage of information before the actual announcement. Due to potential leakage from sealed cases, we also consider alternative event windows starting a few days before the event day and our conclusions remain robust. We note that, by our research design, our estimates are a lower bound of the aggregate market value of trade secrets. This is because we exclude several high-profile cases filed after the news became public (e.g. Yahoo!, AMSC and Equifax) because the DoJ action comes many years after the theft has become public.

We document statistically and economically significant decreases in stock market returns around these events in both relative and absolute terms. Cumulative abnormal stock returns (CARs) range from -1.26% (over the window [-3,+3]) to -1.74% (event window [-4, +1]). It is also informative to describe the impact in absolute terms. The average dollar loss over these two windows ranges from $1.51 billion to $2.09 billion, an order of magnitude larger than the estimate of Searle (2010) ($5 to $250 million). To put this finding in perspective, the value of a theft is larger than a typical Russell 2000 company (mean market cap is about $2 billion). The corresponding aggregate loss in market value in our sample of 72 observations ranges from

$108.9 billion (event window [-3,+3]) to $150 billion (event window [-4,+1]).

To address the question whether the stock market reaction persists more than a week after the announcement, we extend the event window to cover 30 days after each event. We find that the market value loss associated with the trade secret theft does not revert and is even larger than the results reported above. Specifically, the cumulative abnormal stock return (CAR) over the [-5,+30] event window is -2.20%. The corresponding aggregate market value loss from trade secret misappropriation rises to $190.4 billion over this period. We conclude that the estimated value of trade secrets is economically important magnitudes because these firms are very large (and arguably important for endogenous/long-run growth).

Trade secret theft might affect the firm through loss of future revenue and/or higher costs associated with internal investigations, elevated post-event security (including cyber), and/or higher expected litigation and prosecution costs (e.g., De Martinis et al. (2013)). To assess how firms respond to the large shock in market value associated with trade secret thefts, we investigate potential organizational restructuring that may follow in the first three years after misappropriation. We document a tendency of victim firms to engage in acquisitions of smaller firms. The majority of acquisitions take place within the first calendar year after the theft. We interpret this finding as a potential attempt to recover some intangible capital and new intellectual property.

We contribute to a number of related literatures; the measurement of intangible capital and the value of trade secrets, the differences between patents and trade secrets, the association between intellectual property protection and corporate policy, as well as the relationship between intangible assets and cybersecurity risk. We next explain how our paper contributes to each of these areas.

Measuring Intangible Capital Our paper is a part of academic research documenting the increasing importance of intangibles in U.S. firms (e.g. Corrado and

Hulten (2010); Eisfeldt and Papanikolaou (2014); Kogan et al. (2017); Desai et al. (2023); Crouzet and Eberly (2023a)). Despite this increasing importance, estimating firm-level capitalization of intangible assets and their contribution to corporate value is challenging. Unlike physical capital, valuing intangible assets (such as brand, organizational, and knowledge capital) is an imprecise task. Under the US accounting rules, investments aimed at the intangible asset creation are treated as operating expenditures such as selling, general and administrative (SG&A) expenses or research and development (R&D) expenses. As a result, investments flowing into the creation of intangible assets are underestimated and are difficult to separate from other expenditures. Consequently, the majority of intangible assets are excluded from the book value of assets. This could lead to a suboptimal resource allocation (e.g., Kent and Titman (2006)). Recent studies have improved intangible asset estimates by capitalizing prior flows of R&D and SG&A (Ewens et al. (2023)), as well as incorporating intangibles in a classic Fama and French value factor (Eisfeldt et al. (2021)). We contribute to this literature by focusing on the value of intangible capital emanating from trade secrets.

Measuring Value of Trade Secrets In light of the empirical difficulty of observing firms' use of trade secrecy, Lerner (2006) introduces an approach that uses civil court litigation of trade secrecy cases in California and Massachusetts (therefore excluding federal criminal cases) and reports damage awards related to trade secrets averaging $1.5 million. Using 1411 patent infringement cases from the Administrative Office of the U.S. Courts spanning 1983-1999, Moore (2023) finds that the average award for damages is $4.4 million if decided by a judge and $6.5 million if adjudicated by a jury. However, these approaches introduce a sample selection bias; sample firms are confined to appealed cases, excluding privately settled cases and disputes filed under broader categories like contract law. Searle (2010) and Reid et al. (2014) instead use criminal prosecutions under the EEA. These studies use the cost and

revenue model and estimate the damage to the 95 cases convicted during the period of 1996–2008. The estimated damage ranges from $5 to $250 million. This method, however, relies on many assumptions to estimate income generated by trade secrets and investments (or cost) of secrecy and theft protection or damages. We differ from these studies by using the market value rather than book value in measuring trade secrets' value. Our estimate of the market value loss is an order of magnitude larger.

Trade Secrets vs Patents An early theoretical model aimed at understanding the endogenous choice between a patent and a trade secret (Anton and Yao (2004)) predicts that "small inventions are not imitated, medium inventions involve a form of 'implicit licensing,' and large inventions are protected primarily through secrecy." We analyze the empirical connection between trade secrets and patents, documenting that firms own both patents and trade secrets. This correlation becomes stronger as firm size and intangibility metrics grow. Firms that experience trade secret theft are most similar to large firms holding the most valuable patents. These facts are consistent with the (Anton and Yao (2004)) model that small innovations are patented and larger innovations are kept as a trade secret.

Intellectual Property Protection and Corporate Policy Numerous studies use changes in legal safeguards for intellectual property as identification strategies to assess the impact of stricter IP protection laws on various corporate policies. These settings include changes to the Uniform Trade Secrets Act (UTSA), Inevitable Disclosure Doctrine (IDD), non-compete agreements, and additions to the EEA. The effect on a trade secret protection on innovation is un clear. One one hand, it may encourage increase in R&D investment (Samila and Sorenson (2011), Png (2017), and Guernsey et al. (2022)). On the other hand, firms may become less inclined to patent and instead prioritize trade secrecy, indicating that trade secrets can act as a substitute for patents (Png (2017) and Bradley et al. (2023)). The shift toward secrecy could hinder innovation by reducing knowledge spillovers and altering the

nature of R&D conducted by firms. In addition, elevated trade secret protection has been linked to a less conservative financing decision (Klasa et al. (2018), Guernsey et al. (2022)) and a reduction in corporate transparency (Andreicovici et al. (2024)). Firms opt to withhold proprietary information, leading to higher capital costs (Png (2017), Castellaneta et al. (2016), Glaeser (2018), Klasa et al. (2018), Kim et al. (2021)). We contribute to this literature by investigating the effects of trade secret thefts on mergers and acquisitions.

Cybersecurity Risk and Intangible Assets This study is also related to the firm-level ramifications of cybersecurity risk (Kamiya et al. (2021), Florackis et al. (2023), Jiang et al. (2024) among many others). Cybersecurity risk encompasses the potential loss of intangible assets, including trade secrets and data, besides disruptions in business operation network, systems and services. This translates to not only financial loss but also reputational damage. While the firms in our sample are subject to cybersecurity risk, we find that there is minimal overlap with the data breach sample of Kamiya et al. (2021) as they focus exclusively on external cyberattacks. We acknowledge that intangible assets such as trade secrets may be accessed remotely in an unauthorized manner, yet the DoJ cases filed so far focused on individual employees illicitly transferring confidential materials. This differentiates our sample that emphasizes a different aspect of intangible capital.

2 Institutional Background

This section describes the legal background underpinning our data collection, and how we exploit procedural peculiarities to understand the value associated with trade secret thefts.

2.1 Trade Secret Law in the United States

Trade secret misappropriation was primarily governed at the state level until 1979, when the Uniform Trade Secrets Act (UTSA) was introduced to standardize trade secret laws across states; a revision followed in 1985. However, adoption varied across states, creating challenges for large corporations operating nationwide. Furthermore, the U.S. economy's shift towards intangible capital, alongside advancements in IT and increased risks of domestic and international economic espionage, highlighted the need for government action to protect trade secrets and, in turn, national security (e.g., Burstein (2009)). In 1996, Congress enacted the EEA, the first federal law to criminalize trade secret misappropriation. Later, to provide a federal civil cause of action for trade secret protection, President Barack Obama signed the Defend Trade Secrets Act (DTSA) into law.

The EEA defines a trade secret as proprietary information that derives its value from being unavailable to the public and that has to be actively safeguarded. That is, any secret information is eligible for protection as long as its "owner ... has taken reasonable measures to keep such information secret."[9]

The EEA covers a broad spectrum of misconduct, encompassing attempts and conspiracies to acquire trade secrets in an unauthorized manner. More specifically, the EEA criminalizes two forms of proprietary information misappropriation differing in the intent. U.S. Code §1831 defines economic espionage as a transfer of confidential

[9]See "Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act" report by Congressional Research Service, available at https://crsreports.congress.gov/product/pdf/R/R42681.

information to the benefit of foreigners (governments, firms, etc.) and renders it illegal.[10] U.S. Code §1832 specifies that an act of stealing trade secrets with an intent to benefit economically is illegal.[11] Both §1831 and §1832 cover unauthorized theft, possession, concealment, and communication of proprietary information and are not mutually exclusive. For example, an individual is liable under §1832 if he "steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret". However, §1831 requires a proof of foreign involvement and carries potentially higher penalties. Most of the cases in our sample are charged simultaneously under both sections.

Trade secrecy, therefore, stands in stark contrast to patents. Patents must be novel, immediately made public upon filing, while patent infringement is not considered a criminal offense and often settled out-of-court. Trade secrets, on the other hand, are by their very nature concealed and their infringement involves federal criminal charges that can involve sophisticated and costly investigations over a lengthy period of time.

2.2 Federal Prosecution Procedure under the EEA

The legal process usually starts with an official investigation, followed by a criminal complaint if no extra measures are taken to safeguard the company.[12] Typically, law enforcement agencies (such as the FBI) collect data on potential crimes to determine dismissal. If a serious crime with substantial evidence of misappropriation is found, legal proceedings begin. Evidence is submitted for an arrest warrant, executed unless the suspect has fled the country. The DoJ then brings forth criminal charges for EEA violations. A court docket is created upon indictment, often with filing and indictment

[10] https://www.law.cornell.edu/uscode/text/18/1831.

[11] https://www.law.cornell.edu/uscode/text/18/1832.

[12] See an example on how the investigations unfold at https://www.bloomberg.com/news/articles/2023-05-12/the-plot-to-steal-the-secret-coca-cola-can-liner-big-take-podcast.

dates aligning.[13] Details of the case, including victim company name and damages, are promptly made publicly available, sometimes with a press release. At this point, the theft is officially deemed sufficiently severe to warrant criminal prosecution. These indictment dates signify the severity of theft warranting prosecution and form the basis of our empirical analysis. After indictment, legal proceedings leading up to the trial commence, but they are irrelevant to our study.

2.3 Sealed Indictments

The EEA cases inherently involve high complexity, commercial value, and concerns regarding national security. Evidence may include technical drawings and schematics, which upon release, could reveal trade secrets. Under U.S.C. §1835, federal courts can take measures to preserve the confidentiality of trade secrets to the fullest extent during EEA litigation (Levine and Flowers (2015)). Accordingly, federal courts differ in how they announce trade secret cases and their outcomes. Affected firms might not be named directly and are instead referred to as a "Victim Company". In some instances, dockets are sealed to protect law enforcement interests or prevent significant harm to the company, keeping all proceedings confidential as if the case never existed. Later, cases are typically unsealed, making the docket, indictment, and other details available to the public, sometimes in redacted form.[14] In sealed filings, case information is restricted to a limited group of court officials, law enforcement officers, and company insiders. For example, an EEA case involving Apple includes an excerpt stating that

"Because this investigation is continuing, disclosure of the Complaint, this affidavit, and/or this application will jeopardize the progress of this investigation; as such, a disclosure would give the target an opportunity to destroy evidence, change patterns

[13] An indictment is a formal charge by the court indicating that the crime is sufficiently serious and supported by credible evidence, likely leading to a formal trial. A plea agreement, typically involving a "guilty" plea in exchange for a lighter sentence, is an agreement between the defendant and prosecution that bypasses the trial process.

[14] See https://www.uscourts.gov/sites/default/files/sealed-cases.pdf for For the Federal Judicial Center's report of sealed cases.

of behavior, notify confederates or flee from prosecution. Accordingly, I request the Court to issue an order that the Complaint and this affidavit in support of application for the Complaint, be filed under seal until further order of this Court.".[15]

2.4 Sample Construction

2.4.1 Trade Secret Thefts

Our objective is to quantify the value of trade secrets through stock market reactions to trade secret thefts and then understand victims' response. We hypothesize that the market will react strongly and negatively to trade secret thefts, because of the anticipated loss in future revenues. To estimate the potential decline in market value, we need to identify the victim companies and determine when the information has been first disseminated. Therefore, the event dates are essential in our analysis.

Our analysis includes all listed firms in the U.S. over the sample period of 1996 to 2019. For detailed information on EEA court cases, we utilize dockets available at Courtlistener, which contains legal filings associated with each case.[16] The docket usually includes vital information for identifying victim companies and shows how the case unfolds over time (recording court proceedings such as filing dates, indictments, plea agreements, and sealing/unsealing of individual documents or the entire case).

We manually parse legal proceedings and the DoJ announcements to construct the trade secrets theft sample. After identifying victim companies, we must accurately determine the actual "event date" to minimize potential contamination from information disclosed prior to the DoJ case filing. However, not all dockets are complete. Therefore, we impose certain criteria for including EEA cases in our sample. First, we require a full record of court proceedings, including the filing date, indictment, plea agreement, sealing/unsealing status, and all corresponding dates. Second, infor-

[15] For details see
https://storage.courtlistener.com/recap/gov.uscourts.cand.337784/gov.uscourts.cand.337784.1.0.pdf.

[16] Courtlistener, a website offering a collection of legal opinions from federal and state courts, is provided by the Free Law Project, a nonprofit organization affiliated with the Center for Information Technology Policy at Princeton University and Berkman Center at Harvard University.

mation about the victim company must not be redacted; it should be clearly stated and sufficient for identification.[17]

An overview of the case screening procedure adapted from Fang and Li (2021) is outlined below.

1. A case is filed under U.S. Code sections §1831 (Economic Espionage) or §1832 (Theft of Trade Secrets).

2. Its docket is available on Courtlistener.

3. There is only one victim company and it is clearly named. In other words, we exclude cases with multiple victim companies, simply because it is not clear who suffered from the theft.

4. The victim company is publicly listed and primarily traded on a US stock exchange.

5. There are no media mentions of the case predating the filing. We check media mentions using Factiva, Reuters Newswire, Wall Street Journal, and Associated Press. Additionally, we review the US DoJ press releases and archives for any prior disclosure. In other words, we exclude cases if any information about the theft appears in the media before the official case filing.

Using this procedure, we end up with 72 cases, out of the 253 cases reported in Fang and Li (2021). In addition, our estimates of the value loss associated with trade secret theft are likely to be conservative estimates, simply because a number of drastic cases are excluded from our analysis (namely Equifax and AMSC). In the case of Equifax, hackers gained access to private information covering over 140,000,000

[17]For example, consider the following excerpt: "Xu stole and converted to his own use the source code for a piece of proprietary software, which source code was a trade secret of a company for which Xu previously worked." In other documents in the docket, the company is referred to as the "Victim Company". See https://www.courtlistener.com/docket/4356391/united-states-v-xu/ for a full docket.

accounts.[18] The initial public disclosure occurred at some point during the first two weeks of September 2017, but the case was filed in 2020.[19] On September 8, 2017 Equifax stock dropped 13.5%, and bottomed out on September 15 for a cumulative 34.7% loss. We do not include this event because the court case was filed three years after the information became public. Another case is Yahoo! Inc, whose revenue stream was dependent on a trade secret which was stolen. Verizon Communications intended to purchase a substantial part of Yahoo! Inc. for $4.8B before the public announcement of the data theft.[20] The deal was renegotiated, with the sale price dropping by $350M, an estimated drop in firm value equal to 350/4800=7.3%. The AMSC theft is similar to these two cases and we have described it in the Introduction.[21]

2.4.2 Event Dates

In our event study analysis, determining the initial information release date of trade secret thefts is crucial to accurately estimate the value lost. We navigate a series of court dates to establish when the theft is deemed sufficiently serious. We define the event date (day-0) as the earliest of the DoJ filing, indictment, or case sealing date. We classify a case as sealed if its existence or information about the victim firm have been restricted, usually indicated by a motion to seal a criminal complaint and later unsealed. In cases that did not undergo the sealing/unsealing process, the filing date (as indicated by the "Date Filed" field of the Courtlistener docket summary) typically

[18] https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

[19] https://www.courtlistener.com/docket/17149745/united-states-v-zhiyong/.

[20] A bulk of its revenue was generated by the advertisements displayed next to search results or e-mails. For Yahoo!, user data was the most valuable trade secret. However, multiple data breaches between 2014 and 2016 resulted in personal information of over 3 billion users to be compromised resulting in a fundamental loss of trust. The business nosedived, resulting in a sale of most of the assets covering its internet business to Verizon and the re-organization of the remaining part into Altaba Inc. Effectively, Yahoo! went bankrupt and ceased to exist as an independent entity.

[21] It should be noted that there is a selection effect associated with using the EEA cases. Smaller cases will not attract the interest of the federal government due to time, money, and effort necessary for the prosecution.

corresponds to either the indictment or the plea agreement. If sealed, the event date is the sealing date. This accounts for the possibility of insider trading, as company executives privy to the information may transact based on it.[22]

Indictments might come after a sealing date. Nevertheless, on the sealing date, other information can be released that allows us to infer that date. This is illustrated in United States v. HUANG. On June 16, 2010, Kexue Huang, a biotechnology research scientist, was arrested by the FBI and indicted for misappropriating and transporting trade secrets relating to insecticide to China, while employed by Dow AgroSciences. These actions were purportedly intended to enable him and others to compete in the same market as Dow. The case, however, was initially sealed. The DoJ released a press statement on Huang's arrest and charged under the EEA for the first time on July 13, 2010. On August 31, 2010, the case was unsealed.[23] On October 18, 2011, Huang pleaded guilty and ultimately, on December 21, 2011, the court sentenced Huang to 87 months in prison, also for trade secret theft against Cargill (a private company). For this event, the victim firm is Dow Chemical (Ticker: DOW), as Dow AgroSciences is its subsidiary and the event date is June 16, 2010 (the date of Huang's arrest, which is also the sealing date).

2.4.3 Other Data Sources

The financial data are from CRSP/Compustat (merged, accessed through WRDS) and daily stock returns from the Center for Research in Security Prices (CRSP). We obtain patent information from Kogan et al. (2017). Measures of intangibles (knowledge and organizational capital) are based on Peters and Taylor (2017).

[22]In the Online Appendix, we show that sealing dates have similar properties to indictment dates, whereas unsealing dates do not.

[23]The linked document, which was originally sealed, gives a detailed overview of the nature of the theft – Indictment in UNITED STATES of AMERICA v. HUANG court case.

3 Victim Firms

3.1 Trade Secret Thefts by Year and Industry

Table 1 presents a chronological distribution of the 72 trade secret theft cases in our sample, categorized by year, industry, and case publicity status (sealed vs. unsealed). Federal prosecutors invoked the statute in three cases within one year of the EEA's passage. The Clinton and Obama administrations intensified this effort, bringing 34 and 27 criminal trade secret cases, respectively. During the first three years of the Trump administration from 2017 to 2019, the DoJ filed charges resulting in 11 cases, maintaining the previous pace. The cases are fairly evenly distributed chronologically and do not appear to be clustered in specific time periods. Out of 72 cases, 19 were initially sealed.

The sample spans 20 industry categories based on the Fama-French classification. Innovation-oriented sectors, especially those related to military products or high-value personal and company data (such as financial and product development), were frequently targeted. Electronics had 15 cases (e.g., Apple, Intel, Motorola), business services had 11 cases (e.g., Microsoft, IBM), chemicals had 9 cases (e.g., DuPont, Chemours), followed by aircraft with 6 cases (e.g., Boeing). Additionally, pharmaceutical and medical equipment, as well as computers, had 4 cases each (e.g., Bristol Myers Squibb, Cisco).

3.2 Characteristics of Victim Firms

We begin the analysis by examining the firm-level characteristics of our sample that experienced trade secret theft. Table 2 compares summary statistics of various financial and patent variables of the victim firms with all remaining companies. The financial and patent variables are assessed based on the year before the theft to capture victim firm characteristics before potential corporate adjustments due to the

Table 1: **Distribution of Trade Secret Thefts by Year, Industry and Initial Disclosure**

Industry classification is Fama-French 48. Industries without associated cases are not shown. Some names (e.g. "Pharmaceutical Products" listed as "Pharmaceuticals") are shortened. SIC codes are from Compustat Annual. Sealed cases are those that are initially inaccessible (including their existence) to the general public and are made available (existence, parts of the docket, or all materials) at a later date. Number of sealed cases is marked with the "*" and is given in parentheses if different from the total. The total number of sealed and unsealed cases are 19 and 53, respectively.

	Chemicals	**Construction**	**Pharmaceuticals**	**Electronic Eqpt**	**Business Services**	**Machinery**	**Medical Eqpt**	**Banking**	**Computers**	**Communication**	**Defense**	**Candy and Soda**	**Electrical Eqpt**	**Consumer Goods**	**Trading**	**Aircraft**	**Automotive**	**Petroleum, Gas**	**Wholesale**	**Retail**	**Sealed**	**Total**
1997	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
1998	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
1999	0	0	0	1	1*	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4
2000	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
2001	0	0	0	0	0	0	0	1*	2	0	0	0	0	0	0	0	0	0	0	0	1	3
2002	0	0	0	0	1	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	3
2003	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	2
2004	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2005	0	0	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
2006	0	0	0	1	0	0	0	0	0	1	0	1*	1	0	0	0	0	0	0	0	1	4
2007	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	2
2008	0	0	0	3(2*)	2	0	0	0	0	0	0	0	0	0	0	1	1*	1	0	0	3	8
2009	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1*	0	0	0	1	2
2010	2(1*)	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	1	5
2011	1*	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3
2012	1*	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3
2013	0	0	1*	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2
2014	1	0	0	1	1	0	1	0	0	0	0	0	0	0	0	2*	0	0	1	0	2	7
2015	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
2016	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	3
2017	1*	0	0	0	1*	1	1*	0	0	0	0	0	0	0	0	0	0	0	0	1	3	5
2018	0	0	0	2(1*)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	2
2019	0	0	0	1*	1	0	0	0	0	1*	0	0	0	0	0	0	0	1	0	0	2	4
Sealed	4	0	1	4	2	0	1	1	0	1	0	1	0	0	0	2	2	0	0	0	19	NA
Total	9	2	3	15	11	2	4	1	4	3	1	1	1	1	2	6	2	2	1	1	19	72

theft.[24]

Victim firms differ significantly from other firms across various aspects. Victim firms are larger (in terms of market capitalization and assets), more profitable (with higher net income and ROA), have less debt, exhibit higher payouts to shareholders, and make higher tax payments. Interestingly, victim firms do not only rely on trade secrets, but also hold a considerable number of patents, and these patents are extensively cited and very valuable (based on the Kogan et al. (2017) measures).

Figure 2 displays the distribution of intangibles by firms. We match victim firms with other firms by total asset size. In Panel A intangibles are proxied by patent dollar value (Kogan et al. (2017)), and in Panel B intangibles are proxied by total patent citations. For victim firms, the mean patent value (denoted by alternating dots) is 4,918.03M. This mean is economically larger than the mean patent value for comparably-sized non-victim firms, which equals 1,089.08M (denoted by dashed lines). The difference is statistically significant with a p-value <0.0001. We conclude that victim firms have a substantially higher value emanating from intangible assets. This is also confirmed when looking at patent citations. For victim firms, the mean patent citations is 1,230.49M (293.35M for matched firms by asset size). The difference is statistically significant (p-value<0.0001), and also economically substantial.

[24]For example, if the theft occurred in 2015, the comparison is based on the financial data of 2014.

Table 2: **Corporate Characteristics of Victim Firms**

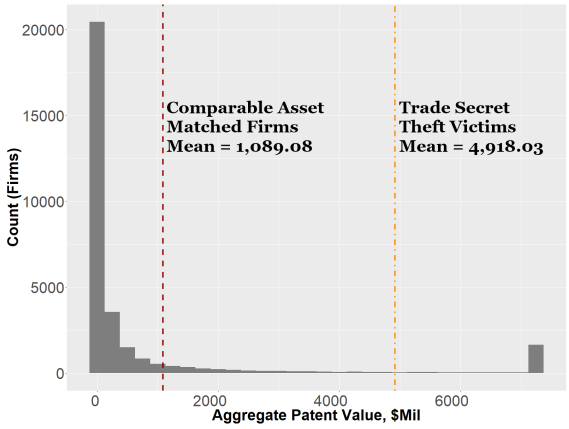
The table presents the means of firm-year financial and patent variables, covering all Compustat firms during the period of 1996-2020. The "Yes" column indicates firms that experienced a trade secret theft in a subsequent year. Market Cap, Assets and Net Income are in millions. Market Cap is in nominal dollars at the time of theft or averaged across all unaffected years. "Patent Value" is the total firm-year patent value in nominal terms. "Patent Citations" is the sum of all patent citations for a given firm-year combination. The patent information is sourced from Kogan et al. (2017). Tail observations (1% from each tail) are winsorized. Two-sample Welch's t-test is used for the comparison between the "Yes" and "No" partitions. ***, **, * denote significance at 1%, 5%, and 10% respectively.

	Trade Secret Theft	
	Yes	**No**
Market Cap.	90,868.9***	4,102.5
Assets	50,697.10***	5,288.30
Net Income	2,156.901***	144.630
R&D Intensity	0.051***	0.070
CAPX	0.042	0.048
Cash Holdings	0.176	0.198
ROA	0.071***	-0.378
Tobin's q	2.370***	4.716
Leverage	0.224***	0.429
Payout	0.057***	0.022
Dividends	0.020***	0.009
Repurchases	0.037***	0.012
Taxes	0.361*	0.260
Physical Invest.	0.260***	0.504
Intangibility	0.808**	0.767
Patent Value	4,918.029***	143.346
Patent Citations	1,230.486***	55.298
Observations	72	163,683

Figure 2: **Distribution of Intangibles: Victim Firms vs. Matched Firms**

The figure displays the distribution of intangibles by firms. In Panel A intangibles are proxied by patent dollar value (Kogan et al. (2017)). In Panel B intangibles are proxied by total patent citations. Alternating dots and dashed lines denote the mean values for victim firms, while dashed lines denote mean values for firms matched by asset size.

Panel A: Patent Value



Panel B: Patent Citations

3.3 Brand Values

Brand values provide additional evidence that firms using trade secrets are large, prominent, and visible companies. We measure brand values using the assessments provided by Interbrand — a management consulting company that issues monetary estimates of the world's top brand values, on an annual basis.[25] We manually match the Interbrand data to our trade secret theft cases, resulting in 16 firm-year observations over the period 2000-2016. This matching allows us to compare brand values of victim firms with other firms.

[25]Current global top 100 estimates can be obtained from https://interbrand.com/best-global-brands/.

Figure 3: **Brand Values: Victims vs. Other Firms**

The figure shows the distribution of brand values (in $ millions) by Interbrand from 2000-2016. The alternating dots and dashes (dashed) line marks the mean brand value of victim (non-victim) firms.

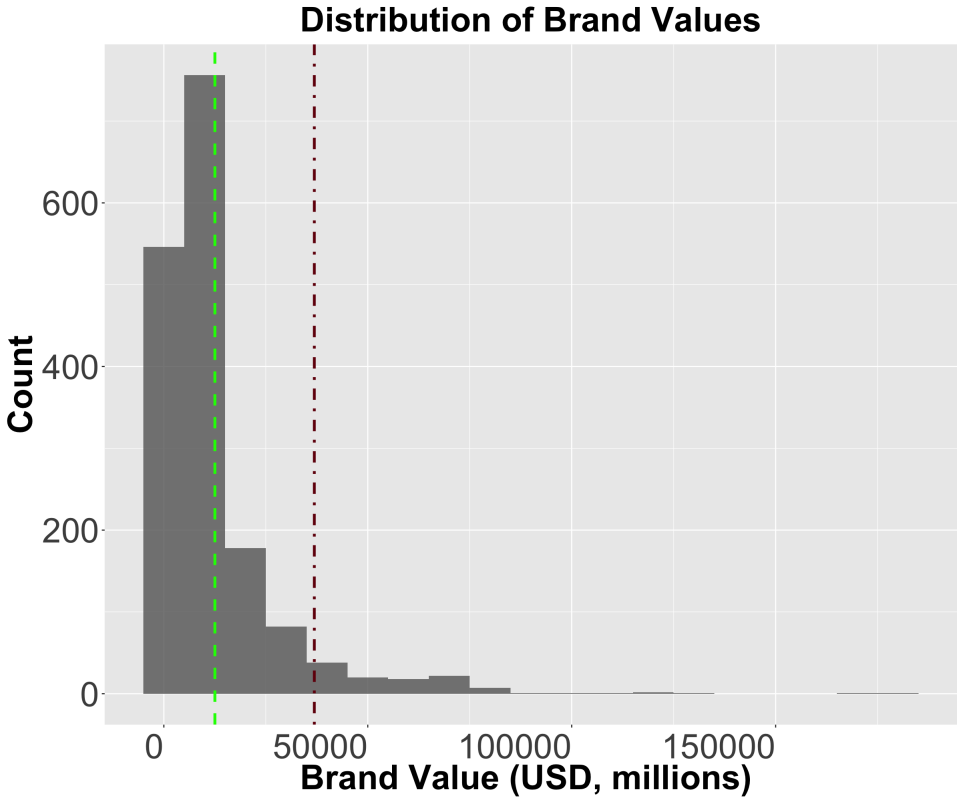


Figure 3 shows the distribution of brand values (in $millions) as assessed by Interbrand over the period 2000-2016. We compare the average brand value of victim firms with the rest. For victim firms, the mean brand value is $36,894.00 million. For the rest of the firms, the mean brand value is $12,519.49 million. Using Welch's Two Sample t-test (which penalizes both small sample size and a difference in group sizes), we compare brand values of the victim firms. The difference between the two is statistically and economically significant with a p-value equal to 0.00125. This result provides further evidence that the companies in our sample experiencing trade secret thefts are prominent and visible. They also rely on (or produce) intangible assets of high value, which are captured by a higher brand value.

3.4 Determinants of Trade Secret Theft

To investigate the correlates of trade secret thefts, we use a linear probability model. The dependent variable is an indicator of trade secret theft set to 1, if a firm experiences a trade secret theft, and 0 otherwise. To mitigate potential concerns about the mis-measurement of intangible capital, we employ multiple measures based on both accounting data (*1-ppent/at* and Tobin's q) and patent metrics (value, citations obtained from Kogan et al. (2017)). Various firm characteristics serve as controls. All variables are measured one year before the theft to account for any potential effects of theft on corporate policy. We also include year and industry fixed effects.

Table 3 shows the results. The two main conclusions are that victim firms are large by asset size and have a high component of intangible value. In regression 1, we use two proxies for intangible assets: accounting intangibility and Tobin's q. The results show that firms with more intangible assets are more likely to experience a trade secret theft. In regression 2 we extend regression 1 by including patent values and citations. Including the patent-based variables makes both the accounting measure of intangibility and Tobin's q statistically insignificant. Nevertheless, the two patent-based variables are strongly statistically significant implying that patents are positively correlated with trade secret thefts.

In regression 3, we incorporate a recursive measure of intangibles from (Peters and Taylor 2017). The recursive measure has three components. First, Total q is a firm's market value scaled by both physical and intangible capital stocks. Second, the fraction of knowledge capital is a portion of intangibles attributed to R&D expenditures divided by a total replacement cost of the firm's intangible capital. Third, the fraction of organizational capital is a share of intangibles attributed to SG&A, divided by an estimated replacement cost of the firm's intangible capital. We follow Peters and Taylor (2017)[26] and keep firms with a positive book equity ($ceq>0$), positive sales ($revt>0$), and sufficiently high (at or above 5^{th} percentile) property, plant and

[26]See "Documentation for data on intangible capital and Total q from Peters and Taylor".

Table 3: **Determinants of Trade Secret Theft**

The table presents estimates from a linear probability model. The dependent variables are indicators set to 1 for firms that experienced theft and 0 otherwise. Observations span 1996-2020. Utilities (4900≤SIC≤4999) and Financials (6000≤SIC≤6999) are excluded. All explanatory variables are measured one year before the theft, and are winsorized (5% from each tail) and are scaled to have zero mean and unit standard deviation. "Fraction Know." and "Fraction Org." are ratios of knowledge (organizational) capital to the estimated replacement cost of firm's intangibles based on Peters and Taylor (2017). "Patent Value" and "Patent Citations" are real value and citations totals using the application date based on Kogan et al. (2017). All regressions control for cash holdings. We describe variable construction in the Appendix. Standard errors are clustered at the same level as fixed effects. ***, **, * denote significance at 1%, 5%, and 10% respectively.

	(1)	(2)	(3)	(4)	(5)	(6)
Intangibility	0.0186***	0.0061	0.0340***	0.0267***	0.0052	0.0375***
	(0.0055)	(0.0049)	(0.0082)	(0.0057)	(0.0046)	(0.0086)
Size	0.1128***	0.0132**	0.1298***	0.1102***	0.0147**	0.1267***
	(0.0149)	(0.0064)	(0.0173)	(0.0145)	(0.0055)	(0.0182)
R&D Intensity	0.0048			0.0145***		
	(0.0033)			(0.0034)		
Tobin's q	0.0412***	0.0035		0.0397***	0.0042	
	(0.0069)	(0.0041)		(0.0054)	(0.0042)	
Patent Value		0.1343***			0.1361***	
		(0.0204)			(0.0251)	
Patent Citations		0.0535***			0.0491*	
		(0.0169)			(0.0261)	
Total q			0.0238***			0.0245***
			(0.0088)			(0.0071)
Fraction Know.			0.0891***			0.0933***
			(0.0170)			(0.0173)
Fraction Org.			0.0387***			0.0336***
			(0.0098)			(0.0096)
Industry FE	Yes	Yes	Yes	No	No	No
Year FE	Yes	Yes	Yes	Yes	Yes	Yes
Adjusted R^2	0.00445	0.00897	0.00496	0.00173	0.00654	0.00266
Within R^2	0.00164	0.00616	0.00237	0.00166	0.00647	0.00258
Observations	134,623	134,160	106,031	134,623	134,160	106,031

equipment (*ppegt*). Total q, the share of knowledge capital, and the share of organizational capital are winsorized at the 5% level. Consistent with the previous findings, the results in column (3) show that all intangibility proxies correlate positively with a higher likelihood of trade secret thefts. For robustness, we rerun regression models 1, 2, and 3 without industry fixed effects. The results in regressions 4–6 are robust; intangibility remains significant regardless of the measure and specification.

4 The Value of Trade Secrets

4.1 Market Reaction to Trade Secret Thefts

We empirically investigate the stock price reaction to EEA prosecutions for trade secret theft using a short-horizon event study analysis, an approach that is "relatively straightforward and trouble-free" according to Kothari and Warner (2007). Following the literature, we use four different specifications to estimate abnormal returns. The simplest model defines abnormal returns as those in excess of the CRSP value-weighted index. The other three models calculate abnormal returns controlling for the CAPM, the Fama and French (1993) three-factor model (FF3), and FF3 including Carhart's (Carhart (1997)) momentum model (FF3 & MOM).[27]

Figure 4 shows the cumulative average abnormal stock market returns (CAAR) several days before and after the event. Over the [-5;5] event window (Panel A), we note a gradual drop in stock prices, starting four days before the event (day-4) and continuing until the day after (day+1). To examine whether the stock market reaction is permanent or transitory, we extend the event window to 30 trading days after the event, as shown in Figure 4, Panel B. The graph suggests that the adverse impact on stock returns is permanent and actually worsens over time. Specifically, we

[27] All calculations are done via WRDS U.S. Daily Event Study. The estimation Window (in days) is set to 252 (corresponds to one calendar year). The required minimum number of returns within the estimation window is set to 188 (corresponds to 9 months). The estimation gap (to prevent model estimation from being affected by the event-induced return variance) is set to 21 days (1 month).

observe an additional, negative stock market reaction starting around seven days after the event (day+7), with a large decline on the eighth day (day+8), and bottoming out 15 days after (day+15). After that, the decline appears to stabilize until the end of the event window. Confidence intervals around the estimates suggest statistical significance over this period.[28]

Table 4 provides further confirmation; average abnormal returns are negative starting four days before the event and ending one day after. The largest one day drop, at -0.686%, takes place two days before the event. Overall, the cumulative average stock price drop is statistically significant and persistent after the event in the sense that we do not observe a reversal in the five days after the event.

Table 4: **Abnormal Stock Returns for Victim Firms around Event Dates**

This table presents abnormal returns relative to the Fama and French (1993) three factor model augmented with the Carhart (1997) momentum. The event window is [-5;5], N=72, and the estimation window is 252 days (one calendar year). The minimum number of returns is 188, and the gap between the estimation and event is set to 21 trading days. "One Sample" refers to the one-sample t-test, "Wilcoxon" is Wilcoxon signed-rank test, "Corrado" is Corrado (1989) rank test. AARs are in percent.

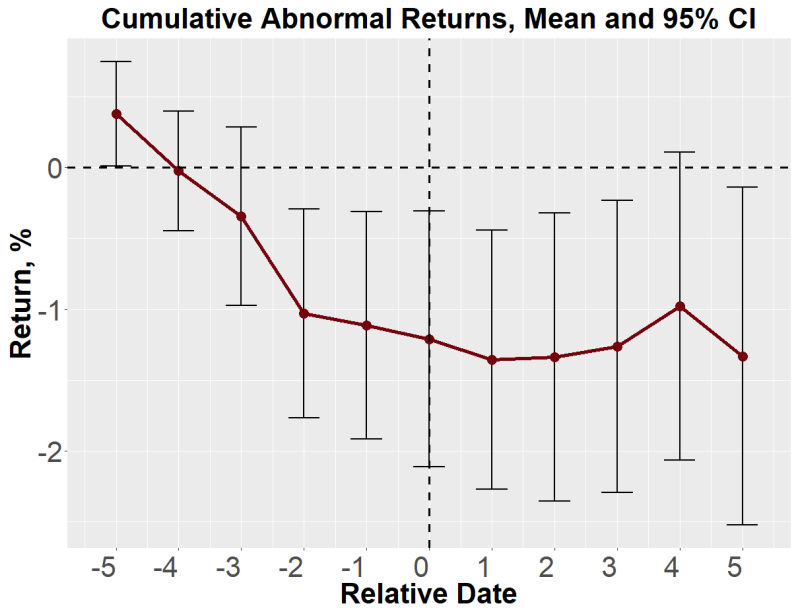
AR (%)		**p-value**		
Day	**Mean**	**t-test**	**Wilcoxon**	**Corrado**
-5	0.375	0.050	0.107	0.077
-4	-0.400	0.009	0.027	0.033
-3	-0.320	0.174	0.033	0.012
-2	-0.686	0.006	0.023	0.020
-1	-0.084	0.686	0.621	0.387
0	-0.096	0.706	0.272	0.173
1	-0.146	0.388	0.154	0.092
2	0.019	0.891	0.850	0.393
3	0.076	0.638	0.876	0.458
4	0.283	0.193	0.689	0.239
5	-0.353	0.243	0.490	0.477

[28]The statistical significance of individual daily abnormal returns is available in the Online Appendix.

Figure 4: **Cumulative Average Abnormal Returns (CAARs)**

Panel A (Panel B) presents cumulative average abnormal stock returns and 95% confidence intervals for victim firms (N=72) over [-5;5] ([-5;30]) event windows. Abnormal returns are estimated using the Fama-French three factor model augmented with the Carhart's momentum (FF3 & MOM) factor.

Panel A



Panel B

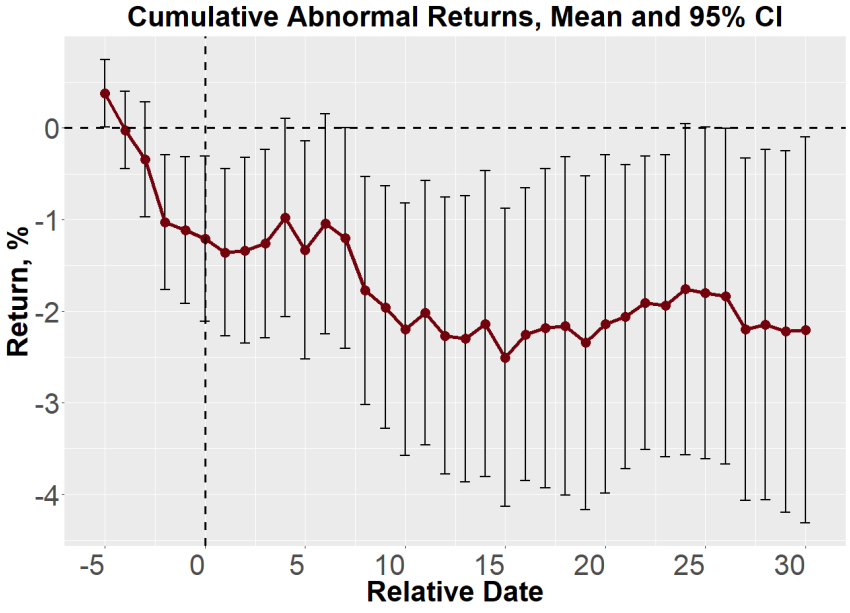


Table 5 presents CAARs based on the four specifications over five different windows. The conclusions from all models are similar in terms of statistical and economic significance. Focusing on the most advanced FF3 & MOM model, the short-term cumulative impact of trade secret loss ranges from -1.26% (event window [-3,+3]) to -1.74% (event window [-4,+1]). Extending the event window to [-5,+30], the cumulative loss amounts to -2.20% indicating no immediate reversal.

In terms of dollar value, the magnitude of the trade secret loss is substantial. Victim firms in our sample have a mean market capitalization at theft of approximately $120 billion (adjusted to 2020 dollars), and are larger than the average S&P 500 constituents. For context, the mean market capitalization of S&P 500 companies on 12/31/2020 was about $64 billion (median $29 billion). The average dollar loss ranges from about $1.51 billion (event window [-3,+3]) and $2.09 billion (event window [-4,+1]). With 72 cases, the total firm value loss ranges from $108.9 billion to $150.4 billion. Over the longer event window, [-5,+30], we estimate the average loss per trade secret theft to be about $2.64 billion. Aggregating over all events in our sample, we estimate the total loss in market value to be about $190.4 billion. Equivalently, over the sample period of 23 years, the average firm value loss is about $8.28 billion per year.

Our findings show that trade secrets are valuable to firms. However, we believe these estimates underestimate the true value of trade secrets. Despite our meticulous identification of the event date, there is a possibility of information leakage, potentially affecting the accuracy of our event date as the first public information release date. Additionally, as noted in Section 2, our sample excludes several high-profile cases that received significant media and market attention before being charged, such as Equifax (which experienced roughly a 34.5% loss in value a few days after the theft) and AMSC (which saw about a 46.4% loss in less than a week after the news became public).

Table 5: **Cumulative Average Abnormal Returns (CAARs)**

This table presents abnormal returns using four specifications: market-adjusted, CAPM, Fama-French three factor (FF3), and FF3 augmented with the Carhart's momentum (FF3 & MOM). Event windows are [-5;5], [-3;3], [-4;1], [-4;-1], [-5;30]; N=72. Presented means are as of the last day (5,3,1, -1, or 30). The estimation window is 252 days, the minimum number of returns is 188, and the gap between the estimation and the event is set to 21 trading days. One-sample t-test is used to compute p-values. CAARs are in percent.

	Market Adj.		**CAPM**		**Fama-French 3**		**FF3 & MOM**	
	Mean	**p-value**	**Mean**	**p-value**	**Mean**	**p-value**	**Mean**	**p-value**
[-5;5]	-1.182	0.104	-1.387	0.033	-1.302	0.040	-1.331	0.032
[-3;3]	-1.463	0.008	-1.434	0.007	-1.348	0.006	-1.261	0.008
[-4;1]	-1.813	0.001	-1.787	0.0002	-1.803	0.0002	-1.741	0.0002
[-4;-1]	-1.656	0.001	-1.506	0.0005	-1.464	0.0004	-1.488	0.0004
[-5;30]	-0.898	0.464	-1.598	0.144	-2.021	0.069	-2.204	0.044

4.2 Insider Trading

If there is value in trade secrets, then insiders will sell ahead of any public disclosures. Anecdotally, as reported by Bloomberg, Equifax executives sold shares after discovering a breach affecting millions of consumers.[29] We therefore investigate whether executives of victim firms sell stocks based on trade secret theft information prior to any public announcement. Our analysis assumes only law enforcement, defendants, and insiders are aware of cases pre-unsealing.

We focus solely on common or preferred stock transactions. We obtain insider ownership and share trading data from SEC Forms 3, 4, and 5, accessible via the WRDS database and EDGAR. Companies must file these forms shortly after any share transaction by insiders, typically within two business days (Form 4). The forms encompass transaction details such as date, price, and volume, and types (e.g., purchase, sale, grant, conversion, hedging or gift).

We implement a filtering procedure to discern insider trades potentially influenced by trade secret thefts, recognizing that some insider trading is routine and some

[29]Bloomberg; September 7, 2017.

is opportunistic in nature (Cohen et al. (2012)). Our method isolates a subset of trades following information dissemination within victim firms but preceding public indictment announcements. The procedure is as follows.

1. All cases come chronologically after the Sarbanes-Oxley Act, which required "real time disclosure" (in most cases, required filing Form 4 within two business days of the trade) and imposed or strengthened penalties for fraud. Since timing is important in this application, "real time disclosure" is a necessary requirement for our analysis.

2. A case must have been sealed and, correspondingly, unsealed.

3. An insider trading form filed with the SEC has two main components: share volume and price, and whether it is a buy or sell.

4. We remove all forms that include a zero transaction price. These are usually Restricted Stock Units (RSUs) grants which are part of the compensation package or discards.

5. We aggregate all filings that have only transactions with positive volume and price over firm-date combinations.

We consider three mutually exclusive time windows. In the first case, we identify all net trades over 7 calendar days (corresponds to 5 trading days) before sealing. In the second case, we identify trades for the time period between the sealing and unsealing dates. In the third case, we look at trades for 7 calendar days after the unsealing dates. There are two measures of interest, net share volume (sum of all shares bought and sold) and net dollar volume ((bought shares*transaction price) minus (sold shares*transaction price)). The results are reported in Table 6.

Regardless of the time period and measure considered in Table 6, all aggregated net transactions are negative. This indicates that, on average, company insiders sell more than they buy when there are trade secret thefts. Specifically, both dollar and

share-valued aggregated transactions are negative and statistically significant over the 7 calendar days before the sealing. At this point, company insiders do not even know whether the case is going to be sealed or even discarded, the decision is generally made at an initial hearing.[30] However, there is an ongoing investigation and employees know that the trade secret has likely been misappropriated and act accordingly.

Table 6: **Insider Trading**

Table 6 includes sealed cases (N=17) after the Sarbanes-Oxley (07/30/2002) Act. Included trades are 7 calendar days (5 trading days) before sealing, or 7 calendar days after unsealing. "Between" is the time period between the sealing and unsealing dates. "Shares" is mean net (buys minus sells) transaction volume (excludes trades with restricted stock units). "Dollars" is mean net (bought shares*transaction price minus sold shares*transaction price) transaction volume aggregated at a transaction (excludes trades with restricted stock units) level. One sample t-test is used to calculate p-values.

		Shares		**Dollars**	
Date	**Trades**	**Number**	**p-value**	**Value**	**p-value**
Sealing	7	–3,548.00	0.001	–223,422.90	0.003
Between	26	–1,077.34	0.812	–411,829.30	0.006
Unsealing	5	–2,584.80	0.484	–327,727.90	0.090

From Table 6 we observe that most of the trades happen in the period between sealing and unsealing. This is the period over which insiders know that the case is important. After all, the case has not been discarded. Moreover, it is deemed to be of sufficient importance to conceal it from the public — hence, it is sealed. Equivalently, the information asymmetry between insiders and general investors is maximized between the sealing and unsealing dates. Unsurprisingly, we see more transactions between sealing and unsealing (26) compared to other periods (7 and 5). Notably, only dollar-valued share sales are statistically significant suggesting the negative information is concentrated in a few, large trades.

[30] See Reagan (2011) for a brief overview of the sealing process, especially as it pertains to the national security issues.

5 Response to Trade Secret Thefts

Previous literature has identified several potential driving factors behind acquisitions including agency challenges (Harford (1999)), overvaluation (Shleifer and Vishny (2003), Rhodes-Kropf and Viswanathan (2004)), synergies (Sirower (1997), Rhodes-Kropf and Robinson (2008), Hoberg and Phillips (2010)), diversification (Markides (1995)), hubris (Berkovitch and Narayanan (1993)) and shocks related to the economy, regulation and technological advancements (Harford (2005)). In this section, we test whether mergers and acquisitions might serve as a recovery strategy in response to a trade secret theft by replenishing intangible capital.

Anecdotal evidence for such a channel exists. For example, PPG Industries acquired Cuming Microwave on June 3, 2015.[31] This acquisition happened one month after the DoJ released trade secret theft charges against Thomas Rukavina, a former PPG employee, for transferring "proprietary and confidential information to J.T.M.G. Co., a glass company based in Jiangsu, China".[32] In the press release, PPG justifies the acquisition as leading to an "enhanced product portfolio" resulting in "innovative and sustainable solutions" and "leadership in innovation". Bower (2001) further emphasizes that for some companies mergers and acquisitions act as a "substitute for in-house R&D" effectively "shortening product life cycles". Moreover, Bower (2001) notes that if "a large player (think GE) is making its nth acquisition of a small company, chances for success go way up", implying that large companies might be tempted to make many small acquisitions.

We consider both domestic and international transactions included in the SDC Platinum database within one, two and three years after the trade secret theft. Table 7, Panel A, shows the accumulated number and value of M&A transactions undertaken by victim firms domestically. The analysis is based on the available deal valuations and reported in 2018 dollars. In all horizons, the total number of acquisitions

[31] See https://news.ppg.com/press-releases/press-release-details/2015/PPG-to-Acquire-Specialty-Coatings-and-Materials-Manufacturer-Cuming-Microwave/default.aspx.

[32] See https://www.justice.gov/opa/pr/former-ppg-employee-charged-theft-trade-secrets.

is high. Within three years after a theft, 35 victim firms (associated with 51 out of the 72 cases) pursue 270 acquisition deals. For 93 deals with transaction value data, the mean transaction value equals $1.87 billion. Interestingly, victim firms engage in acquisitions shortly after the thefts. Within the first year, 25 victim firms (associated with 40 out of the 72 cases) undertake 93 acquisitions. Among these, for the 29 deals with available transaction value data, the mean transaction value is $0.99 billion. During the second year, 8 victim firms (9 cases) pursue 100 acquisition deals. All 65 deals with available transaction value data that occur within the first two years have a mean value of $1.2 billion. Finally, victim firms also pursue cross-border acquisitions. Table 8 shows an increase in the number of deals globally but the deal values are smaller than the domestic ones.

Victim firms can also be acquired (become targets). We observe a much smaller number of deals but the deal values are much larger. Within the first year there are zero transactions, but in the second year two victim firms are acquired. For these cases, the average transaction value for targeted victim firms equals $53 billion, which is much larger than when victim firms acquire other firms. In one case, the victim firm is Rockwell Collins and is acquired by United Technologies for $33.3 billion. The second case is more nuanced because it involves a merger of equals between Du Pont (victim firm) and Dow Chemical and the value is $72.5 billion. In the third year, there is one additional large victim firm that becomes a target with a value of $10.6 billion; Lubrizol is acquired by Berkshire Hathaway.

Table 7: **Victim Firms: U.S. M&A Activity**

The table presents domestic mergers and acquisitions 1, 2, and 3 years after trade secret thefts. All numbers in Panel A are cumulative over the years (except the last column which is an average over the deals with values available). Panel A shows the actual number of transactions, "Acquirer" ("Target") denotes transactions where the victim firm is acting as an acquirer (target), "Cases" denotes the number of theft cases, "Unique Firms" specifies the number of unique companies present in these cases (54 in the entire sample), "Deals" is the number of unique deals, "Deals with value" is the number of deals where deal value is known, "Deal Value" is the average deal value (SDC variable "rankval", in millions of 2018 dollars, adjusted for inflation using the CPI ("FPCPITOTLZGUSA" series)). Panels B and C show a bootstrapped summary of relative significance. Every entry in the table corresponds to a percentile of a Panel A value relative to a bootstrapped empirical cdf. For example, 0.805 (Panel B, "Deal Value" column) should be read as "observed average deal value of $986.87 million is larger than 80.5% of bootstrapped alternatives". Panel B compares the M&A activity to all CRSP firms, Panel C to large (top 5% by capitalization) firms.

Panel A: US M&A, Summary Statistics

	Cases	Unique Firms	Deals	Deals with value	Average Deal Value
Acquirer, 1yr	40	25	93	29	986.87
Acquirer, 2yr	49	33	193	65	1,228.08
Acquirer, 3yr	51	35	270	93	1,873.37
Target, 1yr	0	0	0	0	N/A
Target, 2yr	2	2	2	2	52,890.95
Target, 3yr	3	3	3	3	38,789.24

Panel B: US M&A Percentile, All Firms

	Cases	Unique Firms	Deals	Deals with value	Deal Value
Acquirer, 1yr	1	0.999	1	0.992	0.805
Acquirer, 2yr	1	1	1	1	0.837
Acquirer, 3yr	1	0.976	1	1	0.928

Panel C: US M&A Percentile, Large Firms

	Cases	Unique Firms	Deals	Deals with value	Deal Value
Acquirer, 1yr	0.998	0.421	0.976	0.738	0.023
Acquirer, 2yr	0.997	0.374	0.996	0.923	0.008
Acquirer, 3yr	0.966	0.171	0.994	0.935	0.039

Table 8: **Victim Firms: U.S. and Cross-Border M&A Activity**

The table presents both international and domestic mergers and acquisitions 1, 2, and 3 years after trade secret thefts. All numbers in Panel A are cumulative over the years (except the last column which is an average over the deals with values available). Panel A shows the actual number of transactions, "Acquirer" ("Target") denotes transactions where the victim firm is acting as an acquirer (target), "Cases" denotes the number of theft cases, "Unique Firms" specifies the number of unique companies present in these cases (54 in the entire sample), "Deals" is the number of unique deals, "Deals with value" is the number of deals where deal value is known, "Deal Value" is the average deal value (SDC variable "rankval", in millions of 2018 dollars, adjusted for inflation using the CPI ("FPCPITOTLZGUSA" series)). Panels B and C show a bootstrapped summary of relative significance. Every entry in the table corresponds to a percentile of a Panel A value relative to a bootstrapped empirical cdf. For example, 0.865 (Panel B, "Deal Value" column) should be read as "observed average deal value of $1,202.01 million is larger than 86.5% of bootstrapped alternatives". Panel B compares the M&A activity to all CRSP firms, Panel C to large (top 5% by capitalization) firms.

Panel A: All M&A, Summary Statistics

	Cases	Unique Firms	Deals	Deals with value	Deal Value
Acquirer, 1yr	45	30	141	42	1,052.95
Acquirer, 2yr	53	37	284	84	1,202.01
Acquirer, 3yr	54	38	396	123	1,619.99
Target, 1yr	0	0	0	0	N/A
Target, 2yr	2	2	2	2	52,890.95
Target, 3yr	3	3	3	3	38,789.24

Panel B: All M&A Percentile, All Firms

	Cases	Unique Firms	Deals	Deals with value	Deal Value
Acquirer, 1yr	1	0.999	1	0.999	0.834
Acquirer, 2yr	1	0.998	1	1	0.865
Acquirer, 3yr	1	0.964	1	1	0.933

Panel C: All M&A Percentile, Large Firms

	Cases	Unique Firms	Deals	Deals with value	Deal Value
Acquirer, 1yr	0.994	0.366	0.978	0.766	0.044
Acquirer, 2yr	0.976	0.225	0.988	0.852	0.011
Acquirer, 3yr	0.845	0.051	0.978	0.900	0.035

As previously documented, trade secrets thefts are dominated by large companies with only a few thefts concentrated in a few industries occuring in each year. This makes the acquisitions that arise from these thefts less comparable to the entire population of completed M&A transactions. Moreover, M&A activity is affected by the acquirer size and there is time-dependence in M&As, commonly referred to as "waves" (see Netter et al. (2011)). To determine statistical significance, we employ a bootstrap procedure to compare the relative level of acquisitions and deal size by victim firms with a matched sample (all in 2018 values). The bootstrap procedure is motivated by Harford (2005), who uses a very similar approach to investigate properties of merger waves.

The bootstrap is performed as follows. We take the victim firms sample, fix the dates of the thefts and randomly generate victim firms (pseudo-victims) from the CRSP data base in that specific year. Fixing the dates of theft mitigates the time-dependence (waves) of mergers and acquisitions. To account for the effect of acquirer firm size, we use two different pools for the potential pseudo-victims. The first pool includes all CRSP firms active in a theft year ("All Firms"). The second pool includes only large firms, specifically top 5% by market capitalization at a given year end. We use a 5% cutoff to make results conservative; firms in the "Large" pool are slightly more valuable on average than the firms in the observed affected sample. Larger companies have more resources to acquire (cash holdings, access to both debt and equity financing) so restricting the pool of simulated victims allows us to assess M&A activity controlling for company size — a challenging task when coupled with the time-dependency of data. We repeat the analysis computing the total number and value of acquisitions for each simulated set of victims and repeat the procedure 1,000 times. The results are presented in Figure 5 and Table 7 (Panels B and C).

Figure 5: **Victims' Acquisitions of Other Companies**

This figure displays the number and value of all acquisitions undertaken by the victim firms within one year of a trade secret theft. The reference distribution is generated using the bootstrap by fixing the dates of theft and then randomly assigning pseudo-victim firms. Potential pseudo-victims are drawn from two pools: "All Firms" (all CRSP firms active in a misappropriation year) and "Large Firms" (top 5% by market capitalization). The bootstrap procedure is repeated 1,000 times. The observed sample mean for victim firms is marked with the dashed orange line. The mean of the bootstrapped distribution is in dark red and marked with a dot-dash line.

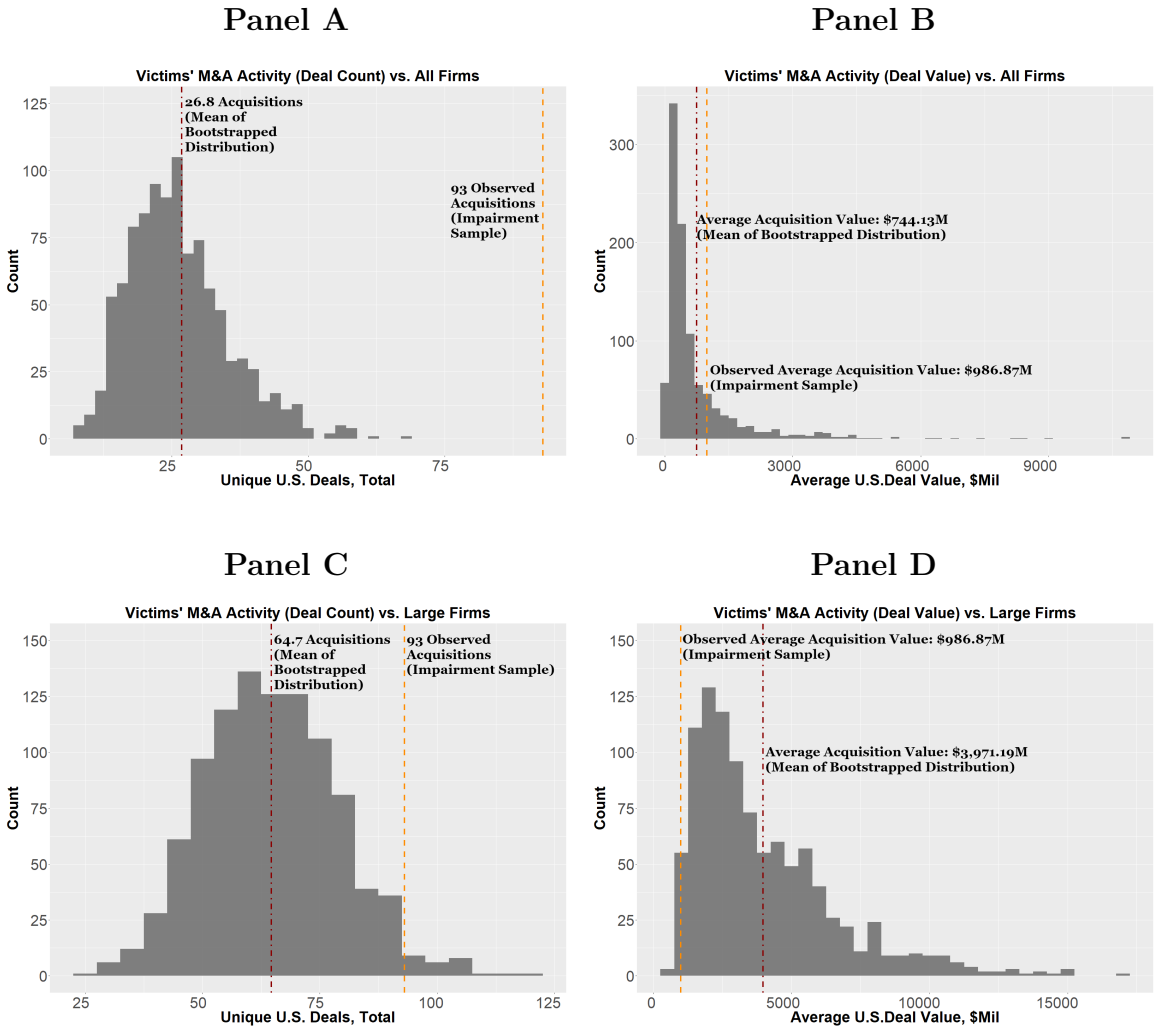


Figure 5, Panel A, compares M&A acquisitions by number of deals for all CRSP firms active in a theft year ("All Firms") with victim firms in that year. There are 93 observed acquisitions for victim firms in the first 365 days after a theft, and these exceed the number of acquisitions expected to be made by an average firm (26.8). This difference suggests that acquisitions are a potential way to quickly secure new intellectual property, a behavior common to large firms. Panel B compares deal values. For victim firms, the average observed deal value is 986.87 million and is higher than the expected value in a given year which equals 744.13 million.

To address size effects, we turn to the "Large" pool (top 5% by market capitalization) to draw potential victims. The results are in Figure 5, Panels C and D. The total number of acquisitions remains much higher than the average across large firms (93 compared to 64.7) but the relative deal valuation declines. The average observed deal value of 986.87 million is smaller than the average purchase of their peer large firms which equals 3,971.19 million.

Table 7, Panel B and Panel C show bootstrapped percentiles. Every entry in the table corresponds to a percentile of a Panel A value relative to a bootstrapped empirical cumulative distribution function. For example, 0.805 (Panel B, "Deal Value" column) should be read as "observed average deal value of $986.87 million is larger than 80.5% of bootstrapped alternatives". Panel B compares the M&A activity to all CRSP firms, Panel C to large (top 5% by capitalization) firms. In both Panels, both the number of deals and the deal values are statistically significant. For instance, compared to all simulations, large victim firms in Panel C are in the 99.8^{th}, 99.7^{th}, and 96.6^{th} percentiles by the number of acquisitions within 1, 2, or 3 years, respectively. Table 8 shows that these conclusions remain unchanged when we extend the sample to include cross-border transactions.

In summary, victim firms make a large number of relatively low-valued acquisitions regardless of whether we focus on 1, 2, or 3 years after a trade secret theft. One potential interpretation is offered by a real options perspective where the low-valued

acquisitions act as options to replenish intellectual property rather than undertaking the original research in house.

6 Conclusion

In this paper, we contribute to the literature by emphasizing the value of trade secrets in intangible capital. We exploit criminal cases filed under the Economic Espionage Act of 1996 that makes theft and misappropriation of trade secrets a federal crime. We hand-collect cases where the announcement of judicial proceedings is likely to be the first public mention of the crime. Victim firms are larger than the average S&P 500 constituent, own highly valued and cited patents and operate in industries associated with dual-use (military and civilian, e.g. aircraft) technology.

Using a short-window event study, we estimate the stock price reaction to trade secret thefts. The estimates range from -1.26% (event window [-3,+3]) to -1.74% (event window [-4,+1]). In absolute terms, these losses are between $1.6 billion to $2.1 billion per case. Extending the event window to [-5,+30], the cumulative loss is -2.20%, with a corresponding dollar value of $2.64 billion average per event. This finding also indicates no immediate reversal for the victim firms. Across all events between 1996 and 2019, the aggregate market value lost is substantial and equals $190 billion. After the theft, victim firms acquire a large number of small companies, perhaps as a recovery strategy.

We emphasize the conservative nature of our estimates. Not all thefts are discovered, assessed, and valued and our estimates do not include diminished competitive standing (at the very least due to a potential new entrant), or lack of spillovers and business ties (for instance, reservations to cooperate with other companies if the intellectual property is damaged). Therefore, we expect the aggregate loss to the economy to be significantly higher than our estimates, in turn adversely affecting economic growth by reducing the incentive to innovate and entrepreneurship more

broadly. Consequently, our results have strong implications for public policy.

References

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

Andreicovici, I., Bormann, S., and Hombach, K. (2024). Trade secret protection and the integration of information within firms. *Management Science*.

Anton, J. J. and Yao, D. A. (2004). Little patents and big secrets: Managing intellectual property. *The RAND Journal of Economics*, 35(1):1–22.

Berkovitch, E. and Narayanan, M. (1993). Motives for takeovers: An empirical investigation. *Journal of Financial and Quantitative analysis*, 28(3):347–362.

Bhattacharya, U. (2014). Insider trading controversies: A literature review. *Annual Review of Financial Economics*, 6:385–403.

Bower, J. (2001). Not All M&As Are Alike—and That Matters. *Harvard Business Review*.

Bradley, D., Hu, D., Yuan, X., and Zhang, C. (2023). Trade secret protection and product market dynamics. *Journal of Corporate Finance*, 83.

Burstein, A. J. (2009). Trade secrecy as an instrument of national security - rethinking the foundations of economic espionage. *Arizona State Law Journal*, 11(4).

Carhart, M. M. (1997). On persistence in mutual fund performance. *The Journal of Finance*, 52:57–82.

Castellaneta, F., Conti, R., and Kacperczyk, A. (2016). Money secrets: How does trade secret legal protection affect firm market value? evidence from the uniform trade secret act. *Strategic Management Journal*, 38(4).

Chan, L. K. C., Lakonishok, J., and Sougiannis, T. (2001). The stock market valuation of research and development expenditures. *The Journal of Finance*, 56:2431–2456.

Cohen, L., Malloy, C., and Pomorski, L. (2012). Decoding inside information. *The Journal of Finance*, 67(3):1009–1043.

Cohen, W. M., Nelson, R. R., and Walsh, J. P. (2000). Protecting their intellectual assets: Appropriability conditions and why U.S. manufacturing firms patent (or not).

Corrado, C. A. and Hulten, C. R. (2010). How do you measure a "technological revolution"? *American Economic Review*, 100:99–104.

Corrado, C. J. (1989). A nonparametric test for abnormal security-price performance in event studies. *Journal of Financial Economics*, 23:385–395.

Crouzet, N. and Eberly, J. (2023a). Intangibles, markups, and the measurement of productivity growth. *Journal of Monetary Economics*, 124:92–109.

Crouzet, N. and Eberly, J. (2023b). Rents and intangible capital: A Q+ framework. *The Journal of Finance*, 78(4):1873–1916.

De Martinis, L., Gaudino, F., and Respess III, T. S. (2013). Study on trade secrets and confidential business information in the internal market. *Prepared for the European Commission*.

Desai, P., Gavrilova, E., Silva, R., and Soares, M. (2023). The value of trademarks. *Available at SSRN*, 4280505.

Eisfeldt, A. L., Kim, E., and Papanikolaou, D. (2021). Intangible value. *Critical Finance Review*, 11(2):299–332.

Eisfeldt, A. L. and Papanikolaou, D. (2013). Organization capital and the cross-section of expected returns. *The Journal of Finance*, 68(4):1365–1406.

Eisfeldt, A. L. and Papanikolaou, D. (2014). The value and ownership of intangible capital. *American Economic Review*, 104(5):189–94.

Ewens, M., Peters, R. H., and Wang, S. (2023). Measuring intangible capital with market prices.

Falato, A., Kadyrzhanova, D., Sim, J., and Steri, R. (2022). Rising intangible capital, shrinking debt capacity, and the U.S. corporate savings glut. *Journal of Finance*, 77(5):2799–2852.

Fama, E. F. and French, K. R. (1993). Common risk factors in the returns on stocks and bonds. *Journal of Financial Economics*, 33:3–56.

Fang, H. and Li, M. (2021). Red scare? A study of ethnic prejudice in the prosecutions under the Economic Espionage Act.

Ferson, W. E., Sarkissian, S., and Simin, T. T. (2003). Spurious regressions in financial economics? *The Journal of Finance*, 58:1393–1413.

Florackis, C., Louca, C., Michaely, R., and Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, 36(1):351–407.

Garfinkel, J. A. (2009). Measuring investors' opinion divergence. *Journal of Accounting Research*, 47(5):1317–1348.

Glaeser, S. (2018). The effects of proprietary information on corporate disclosure and transparency: Evidence from trade secrets. *Journal of Accounting and Economics*, 66:163–193.

Guernsey, S. B., John, K., and Litov, L. P. (2022). Actively keeping secrets from creditors: Evidence from the uniform trade secrets act. *Journal of Financial and Quantitative Analysis*, (7).

Hall, B., Helmers, C., Rogers, M., and Sena, V. (2014). The choice between formal and informal intellectual property: A review. *Journal of Economic Literature*, 52(2):375–423.

Harford, J. (1999). Corporate cash reserves and acquisitions. *The Journal of Finance*, 54(6):1969–1997.

Harford, J. (2005). What drives merger waves? *Journal of Financial Economics*, 77(3):529–560.

Haskel, J. and Westlake, S. (2018). *Capitalism without capital : the rise of the intangible economy*. Princeton University Press.

Hirshleifer, D., Po-Hsuan, H., and Li, D. (2013). Innovative efficiency and stock returns. *Journal of Financial Economics*, 107(3):632–654.

Hoberg, G. and Phillips, G. (2010). Product market synergies and competition in mergers and acquisitions: A text-based analysis. *The Review of Financial Studies*, 23(10):3773–3811.

Horstmann, I., MacDonald, G. M., and Slivinski, A. (1985). Patents as information transfer mechanisms: to patent or (maybe) not to patent. *Journal of Political Economy*, 93(5):837–858.

Howitt, P. (2000). Endogenous growth and cross-country income differences. *American Economic Review*, 90:829–846.

Hu, D., Lee, E., and Li, B. (2022). Trade secrets protection and stock price crash risk. *Financial Review*, 58.

Hvistendahl, M. (2021). *The Scientist and the spy: A true story of China, the FBI, and industrial espionage*. Penguin.

Jiang, H., Khanna, N., Yang, Q., and Zhou, J. (2024). The cyber risk premium. *Management Science*.

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

Kelly, P. (2018). The information content of realized losses. *The Review of Financial Studies*, 31:2468–2498.

Kent, D. and Titman, S. (2006). Market reactions to tangible and intangible information. *The Journal of Finance*, 61:1605–1643.

Kim, Y., Su, L. N., Wang, Z., and Wu, H. (2021). The effect of trade secrets law on stock price synchronicity: Evidence from the inevitable disclosure doctrine. *The Accounting Review*, 96(1):325–348.

Klasa, S., Ortiz-Molina, H., Serfling, M., and Srinivasan, S. (2018). Protection of trade secrets and capital structure decisions. *Journal of Financial Economics*, 128(2).

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

Kothari, S. P. and Warner, J. B. (2007). *Handbook of Empirical Corporate Finance Chapter 1. Econometrics of Event Studies*. Elsevier/North-Holland.

Kuntz, R. L. (2013). How not to catch a thief: Why the economic espionage act fails to protect american trade secrets. *Annual Review of Law and Technology*, 28.

Lerner, J. (2006). Using litigation to understand trade secrets: A preliminary exploration.

Levine, B. L. and Flowers, T. C. (2015). Your secrets are safe with us: How prosecutors protect trade secrets during investigation and prosecution. *American Journal of Trial Advocacy*, 38(3):461–483.

Markides, C. C. (1995). Diversification, restructuring and economic performance. *Strategic Management Journal*, 16(2):101–118.

Miller, C. (2022). *Chip War*. Scribner.

Moohr, G. S. (2002). The problematic role of criminal law in regulating use of information: The case of the Economic Espionage Act. *North Carolina Law Review*, 80(3):853–921.

Moore, K. A. (2023). Judges, juries and patent cases: An empirical peek inside the black box.

Murphy, K. M. and Topel, R. H. (1985). Estimation and inference in two-step econometric models. *Journal of Business & Economic Statistics*, 3:370.

Netter, J., Stegemoller, M., and Wintoki, M. B. (2011). Implications of data screens on merger and acquisition analysis: A large sample study of mergers and acquisitions from 1992 to 2009. *Review of Financial Studies*, 24:2316–2357.

Office of the Intellectual Property Enforcement Coordinator (2013). Administration Strategy on Mitigating the Theft of U.S. Trade Secrets.

Passman, P., Subramanian, S., and Prokop, G. (2014). Economic impact of trade secret theft: A framework for companies to safeguard trade secrets and mitigate potential threats.

Peters, R. H. and Taylor, L. A. (2017). Intangible capital and the investment-q relation. *Journal of Financial Economics*, 123:251–272.

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

Reagan, R. T. (2011). *Sealing Court Records and Proceedings*. DIANE Publishing, Federal Judicial Center.

Reid, G. C., Searle, N., and Vishnubhakat, S. (2014). What's it worth to keep a secret? *Duke Law and Technology Review*, 13:116–161.

Rhodes-Kropf, M. and Robinson, D. T. (2008). The market for mergers and the boundaries of the firm. *The Journal of Finance*, 63(3):1169–1211.

Rhodes-Kropf, M. and Viswanathan, S. (2004). Market valuation and merger waves. *The Journal of Finance*, 59(6):2685–2718.

Romer, P. M. (1990). Endogenous technological change. *Journal of Political Economy*, 98(5):S71–S102.

Samila, S. and Sorenson, O. (2011). Non-compete covenants: Incentives to innovate or impediments to growth. *Management Science*, 57(3):425–438.

Searle, N. (2010). *The economics of trade secrets: evidence from the Economic Espionage Act*. PhD thesis, University of St Andrews.

Shleifer, A. and Vishny, R. W. (2003). Stock market driven acquisitions. *Journal of Financial Economics*, 70(3):295–311.

Sirower, M. L. (1997). *The synergy trap: How companies lose the acquisition game*. Simon and Schuster.

United States Chamber of Commerce (2013). The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement .

US Senate Committee on the Judiciary (2014). Economic espionage and trade secret theft: Are our laws adequate for today's threats?

Appendix

Variable Definitions

This table includes variable definitions. The data are from Compustat (accessed through WRDS), and the "Definition" column uses the Compustat notation. Market capitalization, Assets, Net Income, and Patent Value are all in nominal dollars unless explicitly stated otherwise.

Variable	Definition	Description
Market Cap.	prcc_c*csho	Market capitalization (millions)
Assets	at	Total assets (millions)
Net Income	ni	Net income (millions)
Intangibility	1-ppent/at	Share of non-physical assets
CAPX	capx/at	Capital expenditures
Cash Flow	(ib+dp)/at	Cash flow intensity
Cash Holdings	che/at	Cash holdings intensity
Size	log(at)	Firm size
R&D Intensity	xrd/at	Research and development
ROA	ni/at	Return on assets
Physical Invest.	capx/ppent	Physical investment
Payout	(prstkc+dvc)/at	Cash returned to shareholders
Dividends	dvc/at	Share of dividends
Repurchases	prstkc/at	Share of repurchases
Taxes	txt/ni	Effective corporate tax rate
Leverage	(dltt+dlc)/at	Total debt to assets
Tobin's q	(at-ceq+prcc_c*csho)/at	Ratio of market and replacement values
Patent Value	See Kogan et al. (2017) for a patent-level calculation	Sum of nominal patent values for a firm-year combination (in millions)
Patent Citations	See Kogan et al. (2017) for a patent-level calculation	Sum of patent citations for a firm-year combination