Surprisingly Small:
The Effect of Trade Secret Breaches on Firm Performance

Paper presented to the 2021 Workshop on the Economics of Information Security (WEIS)

June 2021

Nicola Searle[1] and Andrew Vivian[2]

Key words: Event study, trade secrets, breach, cybersecurity, economic espionage, industrial espionage

Abstract: The economic role of trade secrets is expanding but these valuable assets are increasingly the target of theft and cybercrime. As an important strategic resource for firms, the loss of trade secrets should negatively impact the firm. Using an event study for the entire population of publicly listed firms who are named victims in criminal proceedings for trade secrets under U.S. federal law, this paper introduces a new data set to examine the stock market impact of the announcement of a loss of trade secrecy. The study finds there is no statistically significant abnormal return to the announcement overall. However, univariate analysis identifies that R&D intensive firms experience statistically significant negative returns, as do firms with low market-to-book-value ratios. More severe crimes result in negative returns. We find that outsider crimes, high value crimes, and defendants who are corporations also convey more negative returns. The lack of an overall statistically significant abnormal return to stock market prices suggests the theft of trade secrets has become a routine cost of doing business for large firms, and while it is in contrast to much of the IP litigation literature, it aligns with emerging thought in the cybercrime literature.[3]

Introduction

> Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs and more than $1 billion in shareholder equity at AMSC.
>
> Acting Assistant Attorney General Cronan, July 2018 (DOJ, 2018)

[1] Digital Economy Fellow, ICCE, Goldsmiths, University of London; this work funded by Engineering & Physical Science Research Council (EPSRC) Grant EP/P005039/1, Economic Espionage and Cybercrime: Evidence and Strategy.

[2] Professor of Finance, Loughborough University, U.K.

[3] Acknowledgements: The authors would like to thank Jeremy Wu and Ivan Png for the generosity with data. We would also like to thank the anonymous reviews of the 2021 WEIS event for their helpful feedback. We would also like to thank Annsley Merelle Ward.

Industrial and economic espionage are said to cost between 1-3% of GDP in developed countries (Passman, 2014), with companies claiming lost jobs and shareholder equity. Trade secrets, the target of these thefts, are an important protection mechanism for firms and innovation tool for policymakers. While cases such as AMSC claim high losses, there is limited systematic understanding of the stock market performance impact of the announcement of a trade secrets theft. This paper is the first to provide a comprehensive event study on these impact of trade secrets thefts, using the entire population of Economic Espionage Act cases from 1996-2020.

Trade secrets are valuable informational assets for firms and a preferred form of Intellectual Property (IP) protection (A. Arundel, 2001; Cohen, Nelson, & Walsh, 2000; B. Hall, Helmers, Rogers, & Sena, 2014). Technological advances and digitalisation mean that trade secrets are increasingly used, but at the same time more vulnerable to misappropriation and theft through cybercrime. For innovative firms, the loss of trade secrecy through theft can result in lost contracts, competitive advantage and, the subject of this paper, losses to shareholders.

Recent policy interest in trade secrets highlights the growing importance of trade secrets and increased litigation (Almeling, Snyder, & Sapoznikow, 2009). The European Union (EU) (EU Directive on Trade Secrets, 2016) and the US have both enacted major changes to their trade secret laws (Uniform Trade Secrets Act, 2016), alongside a global trend for criminalising the theft of trade secrets. This paper uses American federal criminal court data to investigate the theft of trade secrets and the impact on the firm.

This paper is structured as follows: a literature review of trade secrets and event studies literature, description of the methodology, data analysis, discussion and conclusion.

Literature Review

Trade secrets are a preferred means for firms to appropriate the returns from innovation (Arundel, 2001; Cohen et al., 2000). Trade secrets are knowledge which is: secret, derives value from its secrecy and is reasonably protected. Trade secrets can be extremely valuable (Reid, Searle, & Vishnubhakat, 2014) and are a strategic tool for innovative firms (Arora, Athreye, & Huang, 2016; Crass, Garcia Valero, Pitton, & Rammer, 2019). The secrecy of these intellectual assets means little is known about their use in practice. The theft of trade secrets, in which a trade secret is misappropriated in a manner and jurisdiction that makes it a criminal act, poses a threat to the competitiveness of a firm. The theft of trade secrets also offers unique insights into the use of trade secrets, and their importance in markets.

Trade secret theft is virtually synonymous with industrial, commercial and corporate espionage; when trade secret theft benefits a foreign entity, it is known as economic espionage (Button, 2020). For both firms and economies, such espionage can be a cost-effective, albeit illegal strategy for competitors to innovate by avoiding the costs associated with research & development and fill in missing capabilities (see (Hou & Wang, 2020) for a literature review). For example, systematic economic espionage by East Germany lowered the Total Factor Productivity (TFP) gap between East and West by 13% (Glitz & Meyersson, 2020). In modern times, Western governments are particularly concerned about the rise in malicious, state-sponsored economic espionage (Lucas & Taylor, 2021). A related legally sound strategy for competitors is to engage in competitive intelligence collection (Wright & Roy, 1999), which involves collecting, processing and storing knowledge from the environment to inform a firm's strategy, and falls within the bounds of ethical and legal norms (Rouach & Santi, 2001).

Firm have developed sophisticated litigation strategies to protect their IP and gain competitive advantages. Patent litigation, known as 'the sport of kings' (Rooksby, 2013), is deployed to stop competition, gain royalties, disrupt competition and deter infringement. Firms can use aggressive litigation strategy to reduce litigation risk, improve bargaining positions, establish proprietary rights in niche areas, and increase royalty rates (B. H. Hall & Ziedonis, 2007). Trade secret litigation, perhaps the 'sport of spooks,' can achieve similar goals although requires that the secret is obtained through improper means rather than simply infringement. Civil litigation generally involves the trade secret owner pursuing misappropriation by a third party. This litigation is increasing 14% annually in the US (Elmore, 2016); UK courts have expressed concern about the rising use of confidentiality (of which trade secrets are a subset) claims to shield documents in IP proceedings (Roth, 2019).

Criminal proceedings can be part of a firm's trade secrets litigation strategy. Unlike civil litigation, criminal actions require the involvement of the government. In the US, the first step towards is reporting the theft to the FBI. Firms may choose not to report a theft of trade secrets as they may be embarrassed, worried about loss of goodwill or have business diplomacy concerns. Pursuing action also runs the risk that court proceedings may further reveal the secret and further compromise its value (Argento, 2013; Basuchoudhary & Searle, 2019; Martinis, Gaudino, & Respess III, 2013). Acknowledging the theft of trade secrets may also make firms more vulnerable; discussion of trade secrets in firm filings is associated with an increase in cyber breaches (Ettredge, Guo, & Li, 2018). Criminal actions can be useful in pursuing judgement-proof defendants (i.e. defendants without financial resources to pay potential damages) and do not preclude parallel civil actions (Evans, 2018).

Trade secret theft overlaps with three key areas of event study analysis: IP misappropriation, white-collar crime and cyber breaches. While related relationships between stock market performance and these three areas have been well investigated, analysis of the theft of trade secrets is underdeveloped. This section addresses these topics and the insights they offer for trade secrets.

Patent litigation

Trade secrets are often framed in the literature by their relationship with patents (B. Hall et al., 2014; Reid et al., 2014). Like trade secrets, patents provide legal means for firms to reap the rewards of their innovations. Trade secrets can be used as a substitute or complement to patents; virtually all patents will have been trade secrets at some point. Patent litigation, which is exclusively a civil matter, involves the potential loss of exclusivity of IP, and therefore offers insights for similar losses in trade secrets. Patent litigation strategy is a complex business practice which is influenced by, among others, the contestability of the market, patent values, strategic patenting, court rulings, and joint ventures (Yang, 2019). Patent litigation can involve suing an alleged infringer or filing a patent opposition to dispute the validity of a patent. Like trade secrets, a key uncertainty in patent litigation is the loss of protection; the court may invalidate the patents in question.

Patent litigation is an expensive endeavour and can damage both the patent owner and the alleged infringer (Schliessler, 2015). Event studies find that, despite the high costs and risks to both parties, the plaintiff (patent owner) enjoys positive returns and the defendant (alleged infringer) negative. In the IT industry, the defendant suffers an abnormal return of -2.66% and the plaintiff enjoys a return of 2.55% (Raghu, Woo, Mohan, & Rao, 2008). A study on smartphone litigation confirms positive returns for plaintiffs and negative for defendants, with the interesting exception of the firm Apple. The authors find that Apple's business is sufficiently sensitive to patent litigation that it experiences negative returns regardless of position (Nam, Nam, & Kim, 2015). Other estimates, across all sectors, find lower negative abnormal returns for the defendant of -1.5% (Bhagat, Bizjak, & Coles, 1998) and -0.5% (Bessen & Meurer, 2008). While the magnitude of the returns is disputed, the literature agrees on the signs.

Patent oppositions, in which a third party formally challenges the validity of a patent via the patent office, are core to patent litigation strategies. In these cases, the owner of the pending or granted patent faces the loss of patent protection and the consequent loss of competitiveness. The negative impact of the mere filing of a patent opposition is associated with a -0.30% negative abnormal return for the patent owner – a figure that is even larger for more valuable or tenuous patents (Kruppert, 2017). The resolution of a case, in which the uncertainty around the validity of a patent is resolved, conveys a 1.0% positive abnormal return (Marco, 2011). However, other work finds a lack of statistically significant returns, suggests patent litigation abnormal returns may be short-lived and that the impact of such disputes is fading (Sidak & Skog, 2015); this is in line with trends in cyber-breaches discussed later.

Cyber breaches

The majority of trade secret theft involves cyber crime (Basuchoudhary & Searle, 2019; Georgescu & PWC, 2018; Greiman, 2018). Cyber breaches, in which a firm's cyber security is violated, pose substantial threats to firms as criminals steal data, extract payments via ransomware, block websites and target trade secrets. They can be very costly, both in terms of the direct impact such as loss of business continuity and mitigation, and the indirect costs via long-term loss of goodwill with customers, increased cybersecurity costs and loss of competitiveness. However, the impact on the stock market performance is surprisingly limited.

Event studies in cyber breaches are well established, with many studies finding statistically significant negative abnormal returns but with limited economic impact (Hilary, Segal, & Zhang, 2016). For example, in data privacy breaches, the negative abnormal return is only -0.3% and does not persist (Richardson, Smith, & Watson, 2019). A meta-analysis of 45 studies finds 76% of studies conclude a statistically significant abnormal return, of which the majority find a negative return (positive returns were associated with information security firms) (Spanos & Angelis, 2016). Initially significant abnormal returns on the event day of a privacy breach eventually lose statistical significance (Acquisti, Friedman, & Telang, 2006). However, increased cyber breaches are correlated with a decrease in firm productivity (Makridis & Dean, 2018), suggesting that analyses using different methodologies might provide more insights. Cyber breaches are increasingly become a routine cost of doing business and may already be priced in by efficient markets.

There is a complementary explanation for the muted response of markets to cyberbreaches. (Odlyzko, 2019) argues that 'cybersecurity is not that important.' Comparing the impact of breaches to other disruptions such as natural disasters and military actions, he notes the impact of cyberbreaches pales in comparison. While large and impactful cyberbreaches are bound to occur, the narrative should instead focus on risk management rather than the 'rising tide of hysteria.'

White-Collar Crime

As a financial motivated, commercial crime without violence, trade secret theft falls under the provenance of white-collar crime literature. While data leaks such as the Panama Papers have revealed large scale financial crimes and suggest one in seven firms uses offshore vehicles (O'Donovan, Wagner, & Zeume, 2019); policy makers remain sceptical about the ability of auditors, meant to be a line of defense against money laundering crimes, and to exercise professional judgement (Norton, 2018). These crimes may be common but remain hard to detect.

In theory, the market should punish the perpetrators of white-collar crime; in practice, the picture is mixed. Noting ambiguous results in the two decades prior to their study, (Davidson, Worrell, & Lee, 1994) find no overall significant market reaction to announcement of corporate illegalities. However, they do find a statistically significant reaction on subsets of crime types, including a -0.69% reaction on the day of the announcement a firm has stolen trade secrets. Analysing financial crimes in the banking industry, (Zeidan, 2013) finds a statistically significant negative cumulative abnormal return of -1.51% over a three-day window, but no significant impacts in subsets of the sample.

Comparing white collar crime, which conveys direct and reputational costs, to ‘street crime’ committed by employees, which conveys only reputational costs, (Song & Han, 2017) find no statistically significant difference between the two. They conclude this can be attributed to the perception that employees who commit street crime can be terminated with little impact on the firm. However, the overall effect of corporate crime is a negative stock market performance of -2.48% over a five-day event window.

The parallel with white-collar crime literature to our area of inquiry has its limits as event studies in that literature focus on the perpetrators of such crime, whereas the IP infringement and cyber crime literature tends to focus on victims.

Trade secrets theft

Given the importance of trade secrets and their protection (Almeling, 2012), the loss of competitive advantage arising from the theft of trade secrets should result in negative abnormal returns for the victim firm. A 2001 paper (Carr & Gorman, 2001) provides a first look into the potential stock market impact of the theft of trade secrets. The authors find a negative abnormal return of -0.89% on the day of the event, which is significant at the 5% level. Published five years after the criminalisation of trade secrets in the US, the paper has a relatively small sample size of 11 and consequently has limited power for generalisation. It does, however, find the expected negative relationship between the announcement of trade secrets theft and the stock market, an effect with the authors deem a ‘re-victimization’ of firms.

Since the Carr & Gorman paper there has been virtually no further empirical analysis of the theft relationship. Theoretical models and analyses continue to purport a negative relationship between the two. A single case study analysis finds a dispute between two technology firms, Lexar and Toshiba, lead to cumulative abnormal returns for the plaintiff Lexar of -3.1% but quickly rebounded when the litigation concluded in their favour (Gupta, 2016). One point not as well captured by event studies, is that while the negative abnormal returns may be short-lived the long-term loss of competitiveness may be greater (Andrijcic & Horowitz, 2006). The fast pace of innovation may mitigate this by decreasing the value of the trade secret. Furthermore, the theft of a trade secret does not necessarily translate into the full loss of trade secrecy; the ‘thieves’ may continue to protect its secrecy for their own competitive use.

A closely related area of investigation treats changes in trade secrets laws as an event. The Inevitable Disclosure Doctrine (IDD) is a U.S. state-level law that regulates the mobility of workers. IDD increases the protection of trade secrets by supporting the idea that, for example, a former employee will ‘inevitably disclose’ trade secrets to a new employer, and consequently restrictions such as gardening leave, where an employee is paid but not working, can be enforced. A court ruling which rejects IDD increases employee mobility (Png & Samila, 2013). In contrast, a court confirmation of IDD strengthens trade secrecy, and conveys positive abnormal returns to firms, possibly as a result of decreased competitive risks (Klasa, Ortiz-Molina, Serfling, & Srinivasan, 2018).

Direct analysis of the impact of trade secret theft is scarce, however tying together the trade secret, patent litigation and cyber breach event studies literature suggest that a weak but statistically significant negative abnormal return should be observed from the theft of trade secrets. However, this return may be short-lived. We explore these possibilities in the next sections.

Methodology and Data

This paper takes a novel source of trade secrets event data and matches it to the stock market performance of firms who have suffered the theft of trade secrets. Event studies are an intuitively straightforward method to understand the impact of an unexpected change in circumstances for a firm. Event studies look at a specific event, in this case the announcement of the theft of trade secrets, and the change in the stock market price of the firm. The method identifies the abnormal return of the stock market, with the null hypothesis being that there is no abnormal return (i.e. the stock performed as expected in line with overall market performance in the days surrounding the event.)

Data

Events are identified using the US Public Access to Court Electronic Records (PACER) and supplemented with media reports and Department of Justice (DOJ) press releases. Each of the 94 Federal District Courts are searched individually by the relevant criminal codes (1831 and 1832) to identify the entire population of federal criminal trade secrets cases in the US from 1996 - 2020. This search resulted in 4,000 documents across 214 court cases. A novel database was created after whittling down the documents to 450 key files and then manually coded. Of an initial sample of 115 cases associated with listed companies (companies that have been listed at some point in their existence), 12 are excluded for not being listed at the time of the event (ones that have subsequently been listed, or merged to listed companies or were delisted at the time of the event) or where historical data was unavailable for unidentified reasons. This leaves us with a final sample size of 103 events.

Event dates and Parallel civil actions

The dating of the announcement of the trade secrets theft is through independent media research, cross-checked with the (Wu, 2021)[4] database and civil cases. In most cases, the Wu dates are used. These dates are cross checked with the 12 similar cases in (Carr & Gorman, 2001); while in most cases the difference between our data and (Carr & Gorman, 2001) is four days or less, the difference is 98 or more in three cases. This variance is attributed to different methodologies. Our database uses the first public mention of these cases – which includes media, DOJ press releases and court filings. However, Carr & Gorman use wire and print dates. The advantage of print and wire dates is that the date is associated with the more public acknowledgement of the court case; the advantage of our data is that it is more closely aligned with the event itself.

To identify parallel civil actions, the Png database[5] (on file with author Searle) is used, cross-checked using defendant names with the database and then individually researched to determine whether the civil or criminal action was publicly disclosed first. Five civil actions were identified via the Png database. A second check was also done using internet searching by case which uncovered an additional seven cases, for a total of twelve (14%) of events having a parallel civil cases. In the event the civil action is disclosed first, the case in only eight (10%) events, the date of the announcement of the civil case is used. Parallel civil actions were more common when at least one of the criminal defendants is a corporation. It is possible that the

[4] Dr. Jeremy Wu, retired U.S. federal official and co-founder of the Asian Pacific American Justice Task Force, personally collects and manages a database of EEA cases.

[5] Professor Ivan Png, National University of Singapore, holds a private database of trade secret litigation in US states and kindly shared it with the authors.

announcement of some civil actions may have been missed through this method given that some cases are 20 years old and/or news coverage of the event was limited.

Other crime variables

Event date and parallel action alone can only capture the basics of a firm's trade secrets disputes. To give more context to the events, cases were coded for characteristics of the defendant, the nature and severity of the theft and the value of the trade secrets. Table 1 and Table 2 describes and summarises these additional variables.

The characteristics of the defendant, the alleged perpetrator of the theft, convey information about the potential reputational damage and loss of competitive advantage. The data were coded manually for three dummy variables: whether the defendant was an insider or *outsider* to the firm, whether the case involved foreign agents and whether one or more of the defendants is a corporation as opposed to an individual. Outsider theft may be more serious, as it suggests weak cyber security and IP protection measures; although an insider's familiarity with the trade secrets may result in the loss of more strategic information. In cases where there is the involvement of a *foreign* agent, generally in which the case is framed as benefitting agents overseas, the strategic loss may be more significant to the firm as overseas competition may be stronger and less protected by US jurisprudence. Finally, thefts by corporations (*corp.*) are likely the most severe as the defendant is a competitor with the means to capitalise on the stolen information.

We then address the specifics of the alleged theft and trade secrets involved. Where technical details are stolen, the long-term, strategic loss to the firm is likely higher than when it is only confidential business information such as customer lists and databases. *Computer, value* and *nature* are converted dummies of the categorical or continuous variables described below and in Table 2.

Table 1: Dummy Variable Descriptions

Dummy Variables	
n=103	Dummy =1
Civil [dummy]: 1 where event has a parallel civil action; 0 if not	12
Outsider [dummy]: 1 where defendant is an outsider (e.g. hacker); 0 if insider	23
Corporation (Corp.) [dummy**]**: 1 = case includes at least one defendant or co-defendant that is a corporation; 0 = no corporate defendants	8
Foreign [dummy]: 1 where a foreign agent stood to benefit, 0 if only domestic	55
Manufacturing [dummy]: 1 where SIC is between the 2-digit 20 and 39	75
Technological info (Tech. info.) [dummy]: 1 = technical information, or technical information and confidential business information; 0 = confidential business information	56
Computer [dummy]: 0 if no computer or basic computer skills or unknown; 1 = medium computer skills used (e.g. bypassing secured systems while working there) or advanced computer skills (e.g. hacking)	34
Value [dummy]: geometric mean of up to four USD estimates of the value of the trade secret: those argued in court documents or used by the court in sentencing or an estimation thereof, where available (n=87). 0 if not in top third by value or unknown; 1 = top third in value >= $12m.	28

Nature [0-3]: 0 if unknown, accidental or speculative; 1 if Targeted	56

We capture the nature of theft with two categorical variables measuring the level of computer skills used in the course of the theft and the nature of the theft. Data for these categorical variables stemmed largely from indictments and plea agreements. As noted in Table 2, *computer skills level* is coded 0 to 3 with 0 indicating no details were available (or in a tiny number of cases, the theft did not involve computers) and 3 representing fairly sophisticated approaches such as bypassing security to run a virtual computer. The dummy variable of this separates the sample into medium or advanced computer skills, and those that are not medium or advanced. The *nature of the crime* addresses how the defendant identified and sought the trade secrets. This is coded 0 if unknown. A coding of 1 is when the defendant accidentally access the trade secrets, e.g. stumbles across confidential documents left on a park bench. 2 is when the theft was speculative, meaning that the defendant expected that there were valuable secrets in the data stolen, but not a specific secret. Finally, a 3 represents a targeted theft where the defendant knew of and sought a specific trade secret. The dummy variable separates this into cases that are targeted and those that are not. We would expect a crime involving targeted trade secrets and high computer skills to present a great a loss to the firm as the defendant was more determined.

A final measure of the severity of the theft is an estimate of the *value of the trade secrets* stolen. This estimate is subjective. Court documents were manually coded for valuations of the trade secrets argued during the case. Given that these values were often disputed and different valuation methods result in different values, three measures, where available, were collected as low, medium and high. A second method of collecting valuations was a reverse-engineering method in which the defendant's criminal sentence was cross-referenced with the relevant sentencing guidelines to estimate the value used by the court in sentencing (as in (Zwillinger & Genetski, 2000)). Given that trade secrets are not normally distributed (Reid et al., 2014), the geometric mean of the (up to) four valuations is calculated to provide an estimate of the trade secret. This results in valuations of 87 of the cases in the sample. The trade secrets in question are valuable, with an arithmetic mean of USD$94.8 million and a geometric mean of USD$2.7 million. The *value* dummy variable converts this into the top third (=1) and bottom two-thirds (=0) of values.

Table 2: Continuous and Categorical Variables

Continuous and Categorical Variables			
	Mean	Min	Max
Value of trade secret [number]: geometric mean of up to four USD estimates of the value of the trade secret: those argued in court documents or used by the court in sentencing or an estimation thereof, where available (n=87)	$94.9M	$ 7,500	$ 3.16B
Computer skills level [0-4]: 0 if no computer or unknown; 1 = basic computer skills used in this case (e.g. sending info by email; copy info on a USB) 2 = medium computer skills used (e.g. bypassing secured systems while working there) 3 = advanced computer skills (e.g. hacking)	1.3	0	3

Nature of crime [0-3]: 0 = unknown; 1 = Accidental; 2 = Speculative; 3 = Targeted	2.1	0	3

Firm-level financial and accounting data

Firm-level financial market and accounting data is from Thomson Datastream and presented in Table 3. The accounting data is taken such that it would be available by the event window. Specifically, we take the accounting data 2 quarters prior to the quarter at which the event window starts and also for variables which are for the previous year, these a further 4 quarters earlier. The main variables we collect are book value, net income, operating income, total sales, R&D expense, total intangibles, goodwill and number of employees. The main financial market data we collect is the return index and the market value of the company. This enables us to calculate our main firm specific variables. One important reason why we examine these variables is because the way the market reacts to news may depend upon the nature of the firm involved. Given we have around 100 cases and there can be substantial outliers in the data we calculate the variables of interest and then convert them into dummy variables for analysis.

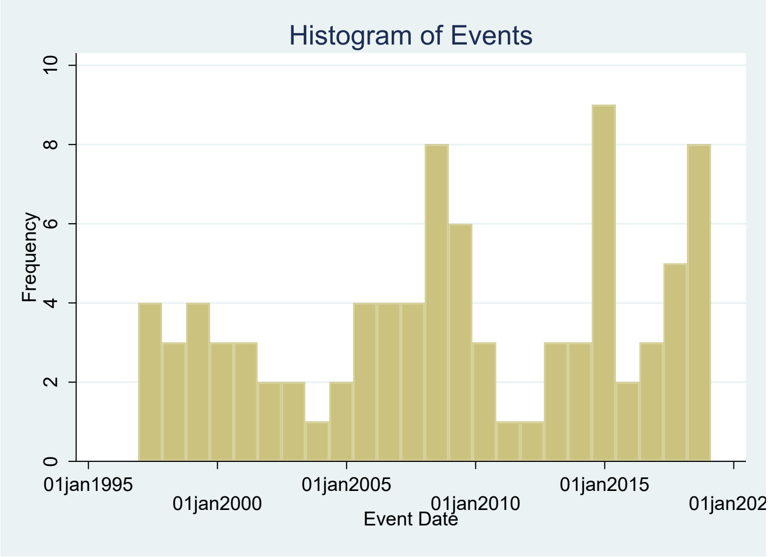
Table 3: Firm-level and financial accounting variables

Dummy Variables	
n=103	Dummy =1
Book to market ratio, BM, [dummy]: calculated as book value divided by the market value of the company at the onset of the event window. We classify firms as 1 if the ratio is above the median; 0 otherwise.	48
R&D intensity [dummy]: this is measured as research and development expense divided by (total) sales. 1 = high R&D intensity defined as a ratio of 10% or higher; 0 otherwise.	37
Sales growth [dummy]: simply the change in sales for the current year divided by the sales revenue in the previous year. 1 = high sales growth defined as sales growth of 10% or higher; 0 otherwise.	34
Employee growth [dummy]: simply the change in sales for the current year divided by the sales revenue in the previous year. 1 = high employee growth defined as 5% or higher; 0 otherwise.	39
Intangible intensity (intang. intensity) [dummy]: calculated as total intangibles divided by total sales. 1 = high intangible intensity defined as a ratio of 20% or higher; 0 otherwise.	46
Residual intangible intensity (res. intang. intensity) [dummy]: calculated as the difference between total intangibles and goodwill scaled by total sales. 1 = high residual intangible intensity defined as a ratio of 10% or higher; 0 otherwise.	32

Distribution

In this section, we present further summary statistics. A histogram of the events, Figure 1, does not show any particular pattern.

Figure 1: Histogram of event dates



In terms of sectors: 75 (72%) are classified as in the manufacturing sector; the remainder are services or banking. Dupont Demours (chemical), and General Electric and its subsidiaries (miscellaneous) are the most popular victim firms with five (6%) cases each. Microsoft (software) has four (4%) cases; the majority of remaining victims are involved in only one (1%) case.

The most popular state for cases is California (29%), with nine in the Central District and 17 in the Northern. The next most popular state is New York (12%), with six in the Southern District, two in the Western and three in the Northern. This distribution reflects the economic distribution of the United States and, in particular, Silicon Valley in California. The Eastern District of Texas, popular for forum shopping patent litigation, is observed only once.

Analysis

The null hypothesis is there are no abnormal returns associated with the announcement of the theft of trade secrets; the alternative hypothesis is that the announcement is associated with abnormal returns to the victim firms' stock.

H_0:μ=0 No abnormal returns

H_1:$\mu \neq 0$ Abnormal returns

The abnormal return is simply the return to the firm experiencing the event minus a measure of expected return. We implement several different specifications to estimate the expected return and generate the abnormal returns. This is because there is currently no consensus in the literature over the most appropriate model. The general specification is shown in equation 1.

Equation 1: Estimating the expected return

$$R_{i,t} = \propto_i + \sum_{k=1}^{k=K} \beta_{i,k} F_{k,t} + \varepsilon_{i,t}$$

Where $R_{i,t}$ is the return to the stock in question of event *i* at time t. We allow for up to K factors to be included whereby $F_{k,t}$ is the return of factor k at time t. and R_t^M is the return to the market at time *t*. The constant is α and the regression coefficient expressed by β. The residual is ε_t and is assumed to be normally distributed. More elaborate models are available, but their advantages are limited (Kruppert, 2017). $R_{t,i}$ is also the observed (actual) return, whereas $\propto + \beta R_t^M$ is the expected (predicted) return.

To calculate the abnormal returns associated with event i at time t, the Market Model looks at the abnormal return $AR_{i,t}$ the difference between the observed return and the expected return, as expressed in Equation 2.

Equation 2: Abnormal Returns in Market Model

$$AR_{i,t} = R_{i,t} - \sum_{k=1}^{k=K} \beta_{i,k} F_{k,t}$$

We use several different specifications to estimate the abnormal return.

Specification 1) Raw return: this specification sets all $\beta_{i,k}$ = 0, thus, $AR_{i,t} = R_{i,t}$,.

Specification 2) Market adjusted return: this specification uses the Market return as the only risk factor (F_1); thus $AR_{i,t} = R_{i,t} - \beta_{i,1} F_{1,t}$

Specification 3) Carhart (1997) 4 factor model: this specification uses the Market return, the Size premium, the Value premium and the Momentum effect.[6]

Specification 4) 5 factor model: this specification uses the Market return, the Size premium, the Value premium, the Profitability effect and the Investment effect.[7]

Please note the data for the return factors are taken from Ken French's data library. We implement equation 2 via the Eventstudy2 package in Stata. The beta coefficients are estimated using time series regressions for each event from 250 days prior to the event up until 30 days prior to the event; this estimation period is used to ensure there are sufficient data points for reasonable estimates but also so that these are not affected by the event itself.

Under the null hypothesis, the mean of AR should be zero. The model is further extended by looking at cumulative abnormal returns (CAR) which is the sum of the abnormal returns during the event window $CAR_{i,t1,t2} = \sum_{t_1}^{t_2} AR_{i,t}$, where the event window is time periods t_1 to t_2, where $t_1 \leq 0 \leq t_2$. We focus on the window from 5 days prior to the event (t-5) to 5 days after the event (t+5) in the empirical tests, i.e. $CAR_{t-5,t+5}$, although we also report initial results over various windows from $CAR_{t-1,t+1}$ up to $CAR_{t-10,t+10}$.

To investigate the overall impact of events – the impact of trade secret theft across the whole population – the average abnormal returns are calculated across N events. These are the average abnormal return (AAR), where $AAR = \frac{1}{N} \sum_1^N AR_{t,i}$ and cumulative average abnormal return (CAAR), $CAAR = \frac{1}{N} \sum_1^N CAR_{t,i}$. The null hypothesis is not rejected if these figures are not statistically different from zero.

[6] Please see Carhart (1997) for a full description of the model.

[7] This model is proposed by Fama and French (2016) where the first 3 factors are from Fama and French (1993) and the last 2 factors are from Hou et al. (2015)

Table 4: CAAR

	Spec. 1	Spec. 2	Spec. 3	Spec. 4
Window	CAAR_raw	CAAR_MA	CAAR_4F	CAAR_5F
[-1,1]	0.21%	0.20%	0.28%	0.17%
[-2,2]	0.29%	-0.03%	-0.12%	-0.19%
[-5,5]	-0.04%	-0.15%	-0.10%	-0.05%
[-5,-1]	-0.52%	-0.20%	0.13%	-0.11%
[0,5]	0.48%	0.05%	-0.23%	0.06%
[-10,10]	0.14%	-0.37%	-0.40%	-0.49%

In Table 4, we report the CAARs using the four different measures of abnormal returns described over 4 different event windows. Interestingly, the CAARs are never more than 0.5% in absolute magnitude. Further, the risk adjustments do not make substantial differences to the CAARs at any event window. For example, for the 21 day event window (t-10, t+10) this has the lowest CAAR of -0.49% for the 5 factor model. Even here the announcement of something as potentially serious as a trade secret breach on average leads to a fall of less than half of one percent in firm value. For the 21 day event window, we see that 4 factor model (which includes momentum) has a -0.40% CAAR while the market adjusted model has a -0.37% CAAR. The only case where CAAR model makes a moderate difference is if purely the raw return is used, in which case the CAAR is 0.14%. If we look at the 11 day event window (t-5, t+5) we see that the CAARs are all very slightly negatively and all very similar to each other; in fact they range from -0.15% (MA) to -0.04% (raw). Economically, this is a tiny margin which is in no way substantially different from 0. Perhaps even more surprisingly, the CAARs turn positive for the 3 day event window (t-1, t+1). However, these range from 0.17% (5F) to 0.28% (4F); once again these are not economically substantially different from 0. We also provide results for the 5 day event window (t-2, t+2); our 2 prime findings continue to hold here: i) the CAAR is (very) close to zero, ii) the risk adjustments do not have at most a moderate impact on the CAAR.

Univariate analysis

Of the univariate analyses, reported in Table 5, the majority as presented are not statistically significant. Only *corporate* is consistently significant across models and tests. *Outsider, value, BM, and R&D instensity* are statistically significant in some models, but drop out (in many cases, only just drop out) in other iterations. We discuss these results below.

Crime Characterisitcs

The first set of variables address the nature of the alleged crime in terms of characteristics of the defedant and aspect of the theft itself.

Civil Cases

The victim firm’s choice to pursue a civil action, in addition to the criminal action, may indicate a more severe crime with a greater impact on the firm. One advantage of the criminal system is that victim firms may pursue retribution against ‘judgement proof’ defendants who lack financial resources. Thus, the pursuit of a parallel civil action may be an indication that the defendant and others involved had more financial means to commercially exploit the trade secret. This represents a bigger potential impact on the victim firm. Under this scenario, the performance of the victim’s stock with parallel civil actions should have a larger, more negative abnormal return compared to cases where only a criminal action is pursued.

Criminal cases have a fairly high 'success' rate compared to observed civil cases. As a benchmark, patent litigation that reaches US district civil courts had a success rate of 33% from 1997-2016 (PWC, 2017). In the 214 cases (1996-2020) in our total database, 60% of cases have at least one defendant who plead guilty. Criminal cases also require less firm resources than civil, as they are not responsible for legal fees.

The sample size for this variable is 11, which is fairly small. The CAARs indicate there is a loss of over 3% when there is a criminal case but a (very) small gain if there is just a civil case. A potential implication of the absence of significance is that the market may not view civil or criminal cases as different, although sample size is likely the dominate influence. We currently lack comparative literature that would allow us to better understand the potential implications of the interaction between the civil and the criminal.

Outsider

We find that whether the defendant is an *outsider* makes a negligible, positive abnormal return for insider cases (0.47% to 0.61%), and a -2.30 to -2.28% return at for outsiders. This is statistically significant at the 10% level under the dummy regression test, but not the rank sum tests. Outsiders represent 22, roughly 20% of our sample. Much of the narrative surrounding the threat of theft focuses on outsiders, so it is not surprising that these events are considered to have a bigger event. An outsider breach also indicates poor external cybersecurity defences, and may suggest that other outsider breaches have gone undetected.

Value of the Trade Secret

To analyse the value of the trade secret, we converted *value* into a dummy where 1 = above the 66th percentile. 28 of our cases fall under this umbrella. Clearly compromised valuable trade secrets should result in more negative abnormal returns. We find a positive but negligible range for low value trade secrets (0.77% to 0.79%) and a negative result response for high value trade secrets (-2.38% to -2.35%). These are significant at the 5% level by the dum reg test, and inside or just outside the 15% level by rank sum. While the valuations we use are imprecise, as indeed are most valuations of trade secrets, they are those as argued in public and therefore should also be accounted for by the market. The data supports this argument – more valuable trade secrets are viewed as greater losses to the firm.

Corporation

The dummy variable *corp* indicates whether one or more of the defendants is a corporation. Thefts by corporation should have more negative impact on the firm as they are typically from competitors and indicate the impact of the theft can be immediately realised as the defendant likely has the capacity to put the stolen trade secrets to use. Our results confirm this, while there is a negligible positive return for defendants who are individuals (0.39 to 0.44%), the return on for corporate defendants is the most negative across our univariate analysis (-7.15% to -6.26%). These are significant mostly at the 5% level (only the p-value of dum reg in Panel B is not, it is instead significant at the 10% level.) Results for this variable should be caveated with the fact that the sample is small, there are only seven cases of corporate defendants.

Technical information

Technical information (*tech info)*, which is trade secrets related to process and product innovations, poses a more strategic threat to a firm's future performance (e.g. competitive advantage). However, non-technical information, such as information related to marketing innovations, organisation innovation or business confidential information (e.g. bids or price lists), tends to be valued higher as the loss of contracts or other competitive advantages can be more immediately assessed. However, despite this framing, we do not find statistically significant results for this variable.

Table 5: Univariate analysis

Panel A:

	CAR_5F [-5;5]	CAR_5F [-5;5]			
			Rank Sum	Dum Reg	
	0	1	p-val	p-val	N=1
Crime					
Civil	0.34%	-3.09%	0.317	0.191	11
Outsider	0.61%	-2.30%	*0.103*	**0.087**	22
Value	0.77%	-2.35%	0.152	**0.038**	28
Corp.	0.44%	-6.26%	**0.038**	**0.068**	7
Tech. info.	0.19%	-0.09%	0.384	0.863	82
Computer	0.31%	-0.31%	0.824	0.975	34
Nature	-0.03%	-0.08%	0.841	0.635	56
Foreign	0.24%	-0.30%	0.702	0.684	53
Firm					
Manufacturing	-0.42%	0.07%	0.490	0.720	73
BM	-1.62%	1.55%	**0.043**	**0.013**	48
R&D intensity	0.66%	-1.20%	**0.084**	0.150	37
Sales Growth	0.16%	-0.44%	0.613	0.679	34
Employee Growth	0.02%	-0.15%	0.959	0.903	39
Intan intensity	-0.95%	0.95%	0.168	0.143	46
Res. Intan intensity	-0.65%	1.18%	*0.119*	0.151	32

Panel B:

	CAR_MA [-5;5]	CAR_MA [-5;5]			
			Rank Sum	Dum Reg	
	0	1	p-val	p-val	N=1
Crime					
Civil	0.32%	-3.85%	0.375	0.153	11
Outsider	0.47%	-2.28%	0.220	**0.093**	22
Value	0.79%	-2.38%	*0.117*	**0.043**	28
Corp.	0.39%	-7.15%	**0.049**	**0.049**	7
Tech. info.	0.23%	-0.22%	0.533	0.757	82
Computer	-0.59%	0.66%	0.205	0.347	34
Nature	0.36%	-0.52%	0.980	0.476	56
Foreign	-0.14%	-0.13%	0.581	0.995	53
Firm					
Manufacturing	-0.02%	-0.20%	0.983	0.871	73
BM	-1.10%	0.81%	*0.130*	*0.133*	48
R&D intensity	0.73%	-1.58%	0.218	**0.084**	37
Sales Growth	-0.17%	-0.11%	1.000	0.962	34
Employee Growth	-0.09%	-0.24%	0.697	0.917	39
Intan intensity	-0.85%	0.62%	0.470	0.246	46
Res. Intan intensity	-0.68%	0.93%	0.369	0.188	32

Notes: This table presents the CAAR over the 11 day window (t-5,t+5) for both the 5 factor model (panel A) and the market adjusted model (panel B). Column 0 presents results when the dummy variable associated with an aspect of the crime or firm is 0, while column 1 provides the value when it is 1. We then provide two tests of statistical significance of the difference in CAAR between when the dummy variable is 0 and when it is 1. Rank sum p-val provides results from the Mann-Whitney non-parametric test of equal value. The Dum reg p-val provides results from a regression of the CAAR on a constant and the dummy variable. We report the two-sided p-value here where a value of greater than 0.1 indicates no statistical difference between the two groups at the 10% significance level.

Computer

The level of sophistication of the cyber crime, as measured by *computer* skills, also does not have a substantial impact on abnormal returns. We would have expected the market to consider more sophisticated thefts to be considered as more serious by the market, but our results do not support that framing. The market could infer that greater cyber more sophisticated skills correlate to more sophisticated criminals with greater potential to use the trade secret to inflict harm on the firm. A counter-argument is that thefts involving lower skills demonstrate poor cybersecurity on the part of the firm, and the market would regard those as more serious. On balance, the two may cancel each other out as we find no evidence to support either take.

Nature of the crime

Like *computer*, more targeted crimes (*nature = 1)* suggest a level of sophistication. Defendants who allegedly targeted specific trade secrets are more likely to have a specific intended use of that trade secret. However, we again do not find evidence to support this framing. In fact, both groups have extremely similar abnormal returns.

Foreign involvement

We also find no impact dependent on whether the theft involves *foreign* agents or not. This conflicts with the wider narrative of economic espionage posing an existential threat. While we would have expected the involvement of foreign agents to have a larger impact than domestic events, the domestic threat is equally as important. In globalised markets, competition from abroad matters, but it may be that a firm's domestic rivals – particularly in a rich country such as the US, are an equal threat. Our results suggest that overall whether there is a foreign agent involved is not a major driver of the market response to the announcement of the theft.

Firm characteristics

Manufacturing

There is much debate as to whether *manufacturing* industries are particularly heavy users of trade secrets. While many studies find high levels of the use of trade secrets in manufacturing e.g. (Cohen et al., 2000), there is minimal study of non-manufacturing firms. An exception is (Morikawa, 2019) who finds similar levels in both manufacturing and services. Another challenge of this literature is that it tends to focus on a subset of trade secrets, namely technical secrets, and neglects the broader spectrum. However, given the literature's general finding that trade secrets are particularly important to manufacturing, we would expect to find a strong negative market reaction to trade secret theft in manufacturing firms. However, the data does not support this.

Book to Market

While the sector does not make a difference (manufacturing or not), the Book Value to Market (*BM*) and R&D intensity do. BM, which is one way to measure the growth potential of a firm (e.g. high BM are in mature industries and low in more dynamic industries). We find that higher BM is associated with a small positive shock on the day of the event (0.81% to 1.55%), which suggests the market sees these more stable firms as being more resilient to trade secret theft. Lower BM instead suggests market expects growth, and therefore the loss of a secret may have a more damning long-term impact, with a range of -1.10% to -1.62%. These are all significant at the 5% or 15% level. The magnitudes of these abnormal returns are relatively modest, but above what we might consider negligible.

R&D intensity

Similarly, we find that *R&D intensity* is statistically significant. The higher the R&D intensity, the greater the negative abnormal returns (-1.58 to -1.20%). Low R&D intensive firms experience a negligible abnormal return of 0.66% to 0.73%. As per Table 5, these are inconsistently significant. R&D intensive firms should also be more dynamic, more innovative firms. Trade secrets are an important mechanism for protecting innovations. Similar to the BM finding, this suggests the market finds the future of these more dynamic firms to be more sensitive to a loss of trade secrets.

Other firm characteristics

Two other measurements of the firm that were not statistically significant were *sales growth* and *employee growth*. While we would have expected high-growth firms to have more, negative abnormal returns because of the potential impact on future growth, this does not appear to be the case.

We also investigate the intangible assets of the firm (*intan. intensity* and *res. intan. intensity* (minus goodwill)). We included these variables to account for the importance of trade secrets as an Intellectual Property Right (IPR) and a means to protect intangible assets. We expected that firms with higher intangible assets would suffer more from a loss as the firm would be a heavier user of IP as a whole, and these IP are often underpinned by trade secrets. The fact that neither of these variables is statistically significant may speak to the diverse nature of trade secrets. The wide scope of trade secrets goes beyond traditional measurements of intangible assets (e.g. number and value of patents, brand value.)

Table 6: Severity of the Crime Indices - Univariate Analysis

Panel A:

						Rank Correl	
	0	1	2	3	4	p-val	Reg p-val
SevIND CAR_5F [-5;5]	1.59%	-0.59%	-3.04%	-6.41%	-9.64%	**0.013**	**0.011**
SevIND CAR_MA [-5;5]	1.42%	-0.30%	-4.30%	-10.00%	-6.97%	**0.038**	**0.011**

Notes: This table reports CAARs for each value of the severity index of the crime (SevIND), which ranges from 0-4. We assess the statistical significance of this variable via two measures. Firstly, a non-parametric test based on Spearman rank correlations and secondly a regression of the CAARs on a constant and the severity index. The p-values correspond to the probability that the null hypothesis that there is no relationship between the CAAR and SevIND under two-sided tests.

Severity of the Crime

Finally, as reported in Table 6, we develop an index to measure an overall impact of the case to provide a single measure of the relevant variables. The index *SevIND* is the sum of the *Civil + Outsider + Value + Corporate* dummies. Across both of these models (5F and MA) we find that there is an increasingly negative abnormal return as the severity of the crime increases. Low severity crimes (0 or 1) have a positive return of 1.42% to 1.59% or negligible negative return of -0.59% to -0.30%. As the level of severity increases, the abnormal return becomes progressively, although not monotonically, more negative, ranging from -10.0% to -3.04%.

These returns are all significant at the 5% level. This indicates that the market behaves generally in the way that we would expect – more severe crimes are interpreted as more damaging to the firm's prospects, which is then reflected in the firm's valuation.

Illustrative case studies

To highlight the dynamics at play, this section develops three cases studies. The cases were selected to present two high profile cases, including the AMSC case referred to at the start of the paper, and one lower profile case. Table 7 contains the values of the key variables related to these cases.

AMSC

As the opening quote of this paper highlights, much attention was given to the impact of the theft of AMSC trade secrets in September 2011. The CAR for this event are -22.37% and -15.35% for the 5 and 11-day windows. Unusually, in this case the defendant is the China-based Sinovel[8], a corporation and not an individual. AMSC sold turbine products and processes to Sinovel, which accounted for three-quarters of AMSC's turnover. Sinovel paid an AMSC employee to give them source code which then the used to in their own turbines. Prior to the case, relationship between the two had started to sour. As of March 2011, Sinovel owed AMSC USD$100M and had contracted to purchase USD$700M of goods and services; in April Sinovel stopped accepting shipments from AMSC[9]. As one of the co-conspirators wrote in an e-mail to another, “"if you succeed, Sinovel can separate from AMSC."[10] That this case is the most dramatic of the cases in our study is not surprising – the victim and the defendant were so entwined that the breakup of the relationship was bound to have negative impacts. AMSC's loss of the exclusivity of its innovations and key customer imposed long-term damage. At the time of writing in 2021, both companies are still in operation although the stock price of AMSC has never reached its pre-April 2011 heights.

Volkswagen

Volkswagen is no stranger to trade secret misappropriation. In 1997, the company paid USD$100M in damages and agreed to purchase USD$1B of auto parts from GM. This settled a civil dispute[11] in which Volkwagen had hired former GM executives who brought GM trade secrets with them (Meredith, 1997). In April 2015, however, the shoe was on the other foot when a court case[12] was filed alleging the theft of Volkwagen trade secrets. The defendant engaged with Volkswagen and Bosch insiders and hired hackers to target the company's trade secrets. The secrets in this case targeting Electronic Control Units (ECU), which can be used to modify a vehicle's performance, and covered technical information and business confidential data, which would enable competitors to produce aftermarket units. The 5-day CAR was -6.46% and 11-day -5.40%. These ECUs are also known as ‘defeat devices' and were involved in the September 2015 Volkswagen emission scandal, in which Volkswagen was found to have manipulated their vehicles for laboratory emissions testing. What is particularly interesting is that this trade secrets case received very little coverage and court documents provide little insights. However, the presence of not one but two scandals associated with the ECU in a short time period suggests that the investigations may have overlapped. Turning over the rock found multiple snakes.

[8] WDWI case number 3:13-cr-00084-jdp

[9] Court document 25, Indictment.

[10] Court document 25, Indictment. P. 8.

[11] This case is civil and therefore not in our database.

[12] SC, 2:15-cr-00236

Apple

Apple was unlucky enough to suffer not one, but two federal cases of criminal theft of their trade secrets in our database. While the thefts themselves were not related, both cases involved trade secrets related to Apple's self-driving car research, and in both cases the trade secrets were allegedly destined to benefit Chinese entities. In the first case on July 09, 2018[13], the CAR are 0.15% and -0.13% for the 5 and 11-day windows. The second event, January 31, 2019, instead has a CAR of 8.22% and 6.32%, again for the 5 and 11-day windows. The key difference between the two is that Apple's stock price had a significant drop at the start of January 2019 after it announced lower projected revenues than expected due to disappointing iPhone sales from longer upgrade cycles and sluggish overseas sales largely due to the slowdown of the Chinese economy[14]. By the time of the event, the stock price was recovering. In this case, it is likely that the nonplussed reaction of the start market to the 2018 event (0.15% and -0.13%) is more representative of the market's assessment of the impact of the theft to Apple's long-term survival. The relatively mild impact is in contrast to (Nam et al., 2015)'s finding that Apple's sensitivity to patent litigation results in a negative response regardless of whether Apple is a plaintiff or defendant. It may speak to the relatively amorphous nature and high levels of uncertainty of trade secrets in contrast to patents.

Table 7: Case study firm – details.

Event ID [Integer]: A unique event identifier.	189	193	217	172
Firm ID [String]: The ticker ID.	AMSC	AAPL	AAPL	VOW
Market ID [String]: The reference market ID.	NAS	NAS	NAS	DAX
Event Date [30.04.1997]: Date of the event.	14/09/2011	31/01/2019	31/01/2019	15/04/2015
Civil	1	0	0	0
Outsider	0	0	0	1
Value	1	0	.	0
Corp.	1	0	0	0
SevIND	3	0	0	1
Tech. info.	1	1	1	1
Computer	0	1	1	0
Nature				
	1	1	0	0
Foreign	1	1	1	0

Findings

That the overall stock market to reaction to the announcement of the theft of a firm's trade secrets is not statistically significant is both surprising and not. In contrast to the extensive literature demonstrating the value of trade secrets and their importance to the competitiveness of the firm, but in keeping with cybercrime understandings, the market appears instead to treat the loss of such assets as relatively mundane.

[13] NDCA case number 5:18−mj−70919−MAG

[14] Apple Press release, "Letter from Tim Cook to Apple investors," January 2, 2019, accessed June 4, 2021 from https://www.apple.com/uk/newsroom/2019/01/letter-from-tim-cook-to-apple-investors/.

Overall impact

The IP literature, both patent and trade secrets, provides nuance to our findings. The patent literature finds positive returns to the plaintiff in patent *infringement* disputes, however this differs from our data in that these are civil suits and the plaintiff can receive significant financial damages as a result. The possibility that a dispute results in the invalidity of the patent (hence the 'victim' firm's loss of patent protection) is present in infringement disputes, but more so in patent *oppositions*. This threat of loss aligns better with the threat of loss from our trade secrets thefts, therefore the findings of minimal impact (-0.3% by (Kruppert, 2017)) or no statistically significant returns (Sidak & Skog, 2015) from oppositions also support our findings. On balance, we find our results in keeping with oppositions literature but not patent litigation literature.

As discussed, the trade secret loss event studies research is limited by small sample size, but both papers identified (Carr & Gorman, 2001; Gupta, 2016) find negative results. Looking at the other side of the issue – expansion instead of loss - the strengthening of trade secrets laws conveys positive returns (Png & Samila, 2013). Long-term strategic losses may be poorly captured by the methodology (Andrijcic & Horowitz, 2006), but this could be tempered by fast-moving technological change in which the market value of a trade secret diminishes over time. Given the weaknesses in the sample size of the existing trade secrets loss literature and the lack of response found by the patent opposition literature, our findings, on balance, are supported by the existing IP literature.

The cybercrime literature also generally supports our findings of a minimal response to theft with limited statistical significance (Acquisti et al., 2006; Richardson et al., 2019), although a literature review concludes most studies find a negative but not dramatic result (Spanos & Angelis, 2016). The minimal response can be explained by (Odlyzko, 2019)'s assertion of the lack of importance of cybersecurity. Equally, the market may have already priced in the expectation of such breaches. The breaches in our population are not glamorous external hacks, but general rather mundane breaches by insiders. The banality of such crimes could be seen as a relatively more damning account of a firm's cybersecurity – that internal controls are so low even unsophisticated breaches are successful. Yet our data does not support such a framing. Instead, our analysis supports the section of the cybercrime literature that finds negligible or no statistically significant abnormal returns.

The white collar crime literature, like the other literature, also finds a mix of negative abnormal returns (Song & Han, 2017; Zeidan, 2013) or no abnormal returns (Davidson et al., 1994). However, we would have expected our findings to be in line with the negative findings of the more recent literature rather than the lack of abnormal returns in the older literature. This literature is more removed from our sample as it focuses on perpetrators and not victims.

Given the emphasis on the emphasis of trade secrets as a strategic tool and the importance of good cybersecurity, we would have expected to find statistically significant, negative abnormal returns in our data. However, our review of the event studies literature in IP, cybercrime and white-collar crime indicated it has not reached a consensus, with no conclusion between the two common findings of negative abnormal returns or a lack of statistically significant returns. Findings of negative abnormal returns are more common, although this could be the result of publication bias. We find the theft of trade secrets aligns to findings of no statistically significant returns. While this is not the case in some individual events, such as the AMSC case study presented, the overall story is that trade secrets and their cybertheft may not be that important to public companies as a whole.

Specific Characteristics

While our overall findings are not statistically significant, we do find statistically significant negative abnormal returns for the severity of the crime, outsider crimes, high value crimes, and defendants who are corporations. The lack of statistically significant results for other variables is less intuitive, although fitting with the overall lack of abnormal returns. The sample size matters as some of our dummy variables have few observations equal to one. Our data captures the entire population of these cases, therefore expansion of the sample size of characteristics at the time of writing is not possible.

We find firms with higher R&D intensity suffer more negative returns as do firms with lower BM. These are both intuitive findings. R&D active firms are heavier users of trade secrets (Morikawa, 2019) and more likely to be innovative. Trade secrets are used throughout the R&D process, particularly in protecting processes and pre-patent innovation; the loss of trade secrets to R&D intensive firms likely represents a greater loss than to a less innovative firm. The BM ratio is along the same lines. Firm with high BM are generally in mature industry, e.g. utilities and food retailers, and have modest growth prospects. In contrast, low BM firms tend to be in exciting, high growth areas. These more dynamic firms may also be more innovative and the shock of the trade secret theft represents a bigger strategic loss.

Our findings point to a market that has generally accepted the loss of trade secrets as a cost of doing business, although such loss poses a greater threat to more innovative firms with higher growth potential. More severe crimes translate to greater losses.

Conclusion

We have shown that there is a limited relationship between the announcement of the theft of trade secrets and the victim firm's stock market performance. While this finding is jarring when contrasted with IP literature overall, it is in keeping with findings in cybercrime, patent and white-collar crime research. We find statistically significant, negative abnormal returns for high growth firms (as measured by BM) and R&D intensive firms, along with more severe crimes.

For policy makers, the implication is the narrative of trade secret theft as a fundamental threat to a country's economy and innovation (in our case, the US), may simply be rhetoric when contrasted to the market's understanding of such theft. While certainly some cases had significant negative impacts on the firm, e.g. AMSC, the overall picture is nothing as dramatic. Therefore, calls for the expansion of trade secrecy protections, such as the expansion of its definition or further criminalisation of trade secret theft, may do less to protect innovation overall and instead expand negative externalities such as increased litigation and constraints on labour mobility.

For managers, the implication is that the benefits of the protection of trade secrets may be overstated. Counterintuitively, the findings suggest managers should *not* prioritise trade secret protections and cybersecurity if the main goal is protecting shareholders. In addition to savings, this has the added benefit of allowing information to flow more freely within the firm, which is conducive to increased firm innovation (King, 2007). Yet dramatic cases, such as AMSC, with significant negative abnormal returns evidence the risk and potential consequences of trade secret breaches. Trade secrets are also only one part of a wider IP system, and the relationships between trade secrets and other IPR are poorly understood. By focusing on the market's response, the methodology used here may not fully capture the longer-term strategic loss when a trade secret is compromised. Managers should take this into account.

The analysis highlights a number of areas for future research. An obvious next step is to focus solely on civil cases, although this will be difficult given data availability challenges (Risch, 2019). The overlap between these trade secrets cases and patent cases may also provide some insights into these two related IPR; this may be possible as large American firms appear to be increasingly pursuing civil trade secret actions against each other. As other jurisdictions criminalise the theft of trade secrets, e.g. Mexico and Canada, there may be further opportunities for a similar analysis.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Almeling, D. S. (2012). Seven reasons why trade secrets are increasingly important. *Berkeley Technology Law Journal*, 1091–1117.

Almeling, D. S., Snyder, D. W., & Sapoznikow, M. (2009). A statistical analysis of trade secret litigation in federal courts. *Gonz. L. Rev.*, *45*, 291. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/gonlr45&id=295&div=13&collection=journals

Andrijcic, E., & Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk Analysis*, *26*(4), 907–923.

Argento, Z. (2013). Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation. *Yale JL & Tech.*, *16*, 172.

Arora, A., Athreye, S., & Huang, C. (2016). The paradox of openness revisited: Collaborative innovation and patenting by UK innovators. *Research Policy*, *45*(7), 1352–1361. https://doi.org/10.1016/j.respol.2016.03.019

Arundel, A. (2001). The relative effectiveness of patents and secrecy for appropriation. *Research Policy*, *30*(4), 611–624. https://doi.org/10.1016/S0048-7333(00)00100-1

Basuchoudhary, A., & Searle, N. (2019). Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets. *Computers & Security*, *87*, 101591.

Bessen, J. E., & Meurer, M. J. (2008). The private costs of patent litigation. *Boston University School of Law Working Paper*, (07–08).

Bhagat, S., Bizjak, J., & Coles, J. L. (1998). The shareholder wealth implications of corporate lawsuits. *Financial Management*, 5–27.

Button, M. (2020). Editorial: economic and industrial espionage. *Security Journal*, *33*(1), 1–5. https://doi.org/10.1057/s41284-019-00195-5

Carr, C., & Gorman, L. (2001). The revictimization of companies by the stock market who report trade secret theft under the Economic Espionage Act. *The Business Lawyer*, 25–53.

Cohen, W., Nelson, R., & Walsh, J. (2000). Protecting their Intellectual Assets: Appropriability conditions and why firm patent and why they do not in the American manufacturing sector. *NBER Working Paper*, *7552*.

Crass, D., Garcia Valero, F., Pitton, F., & Rammer, C. (2019). Protecting Innovation Through Patents and Trade Secrets: Evidence for Firms with a Single Innovation. *International Journal of the Economics of Business*, *26*(1), 117–156. https://doi.org/10.1080/13571516.2019.1553291

Davidson, W. N., Worrell, D. L., & Lee, C. I. (1994). Stock market reactions to announced corporate illegalities. *Journal of Business Ethics*, *13*(12), 979–987. https://doi.org/10.1007/BF00881667

DOJ. (2018). Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets. Retrieved from Department of Justice Office of Public Affairs website:

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

Elmore, J. (2016). A Quantitative Analysis of Damages in Trade Secrets Litigation. *Willamette Forensic Analysis Insights*, *Spring*.

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

Evans, M. (2018). Effectiveness of Available Civil Remedies as a Factor Influencing Prosecution of Economic Espionage Act Cases. *Washburn LJ*, *57*, 463.

Georgescu, A.-A. E. P., & PWC. (2018). *Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber*. Retrieved from https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

Glitz, A., & Meyersson, E. (2020). Industrial espionage and productivity. *American Economic Review*, *110*(4), 1055–1103.

Greiman, V. (2018). Cyber Espionage: The Silent Crime of Cyberspace. *ICCWS 2018 13th International Conference on Cyber Warfare and Security*, 245. Academic Conferences and publishing limited.

Gupta, R. Sen. (2016). Economics of Survival Post Trade Secret Misappropriation: Business Insights from Single Firm Event Study on Lexar Media. *Journal of Advanced Research in Law and Economics (JARLE)*, *7*(17), 521–534.

Hall, B. H., & Ziedonis, R. H. (2007). An empirical analysis of patent litigation in the semiconductor industry. *University of California at Berkeley Working Paper*, 217–242.

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

Hilary, G., Segal, B., & Zhang. (2016). Cyber-Risk Disclosure: Who Cares? *Georgetown McDonough School of Business Research Paper No. 2852519*.

Hou, T., & Wang, V. (2020). Industrial espionage – A systematic literature review (SLR). *Computers & Security*, *98*, 102019. https://doi.org/https://doi.org/10.1016/j.cose.2020.102019

King, A. W. (2007, January 1). Disentangling interfirm and intrafirm causal ambiguity: A conceptual model of causal ambiguity and sustainable competitive advantage. *Academy of Management Review*, Vol. 32, pp. 156–178. https://doi.org/10.5465/AMR.2007.23464002

Klasa, S., Ortiz-Molina, H., Serfling, M., & Srinivasan, S. (2018). Protection of trade secrets and capital structure decisions. *Journal of Financial Economics*, *128*(2), 266–286. https://doi.org/10.1016/J.JFINECO.2018.02.008

Kruppert, R. (2017). Dispute the patent, short the stock: Empirical analysis of a new hedge fund strategy. *International Review of Law and Economics*, *50*, 25–35.

Lucas, R., & Taylor, T. (2021). Sealing Technology Transfer Leaks. *The RUSI Journal*, 1–16. https://doi.org/10.1080/03071847.2021.1896954

Makridis, C., & Dean, B. (2018). Measuring the economic effects of data breaches on firm outcomes: Challenges and opportunities. *Journal of Economic and Social Measurement*, *43*(1–2), 59–83. https://doi.org/10.3233/JEM-180450

Marco, A. C. (2011). The Value of Certainty in Intellectual Property Rights: Stock Market Reactions to Patent Litigation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.945009

Martinis, L. de, Gaudino, F., & Respess III, T. S. (2013). Study on Trade Secrets and Confidential Business Information in the Internal Market. *Prepared for the European Commission*. sn.

Meredith, R. (1997). VW agrees to pay GM $100 million in espionage suit. *New York Times*, A1.

Morikawa, M. (2019). Innovation in the service sector and the role of patents and trade secrets: Evidence from Japanese firms. *Journal of the Japanese and International Economies*, *51*, 43–51. https://doi.org/10.1016/j.jjie.2018.10.003

Nam, S., Nam, C., & Kim, S. (2015). The impact of patent litigation on shareholder value in the smartphone industry. *Technological Forecasting and Social Change*, *95*, 182–190. https://doi.org/10.1016/j.techfore.2015.01.015

Norton, S. D. (2018). Suspicion of money laundering reporting obligations: Auditor compliance, or sceptical failure to engage? *Critical Perspectives on Accounting*, *50*, 56–66. https://doi.org/https://doi.org/10.1016/j.cpa.2017.09.003

O'Donovan, J., Wagner, H. F., & Zeume, S. (2019). The Value of Offshore Secrets: Evidence from the Panama Papers. *The Review of Financial Studies*, *32*(11), 4117–4155. https://doi.org/10.1093/rfs/hhz017

Odlyzko, A. (2019). Cybersecurity is not very important. *Ubiquity*, *2019*(June), 1–23.

Passman, P. (2014). *The Economic Impact of Trade Secret Theft.(CREATe. org)*.

Png, I. P. L., & Samila, S. (2013). Trade secrets law and engineer/scientist mobility: Evidence from "Inevitable Disclosure." *WP Nat. U. Singapore*.

PWC. (2017). *2017 Patent Litigation Study Change on the horizon?* Retrieved from http://www.pwc.com/us/en/forensic-services/publications/assets/2017-patent-litigation-study.pdf

Raghu, T. S., Woo, W., Mohan, S. B., & Rao, H. R. (2008). Market reaction to patent infringement litigations in the information technology industry. *Information Systems Frontiers*, *10*(1), 61–75.

Reid, G. C., Searle, N., & Vishnubhakat, S. (2014). What's It Worth to Keep a Secret. *Duke L. & Tech. Rev.*, *13*, 116.

Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much ado about nothing: The (lack of) economic impact of data privacy breaches. *Journal of Information Systems*, *33*(3), 227–265. https://doi.org/10.2308/isys-52379

Risch, M. (2019). Empirical methods in trade secret research. In *Research Handbook on the Economics of Intellectual Property Law*. Edward Elgar Publishing.

Rooksby, J. H. (2013). When Tigers Bare Teeth: A Qualitative Study on University Patent Enforcement. *Akron L. Rev.*, *46*, 169.

Roth, M. J. (2019, November 19). Infederation Ltd v Google LLC & Ors [2020] EWHC 657 (Ch) (18 March 2020). Retrieved March 27, 2020, from England and Wales High Court (Chancery Division) website: https://www.bailii.org/ew/cases/EWHC/Ch/2020/657.html

Rouach, D., & Santi, P. (2001). Competitive Intelligence Adds Value:: Five Intelligence Attitudes. *European Management Journal*, *19*(5), 552–559. https://doi.org/https://doi.org/10.1016/S0263-2373(01)00069-X

Schliessler, P. M. (2015). Imported from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3474200. *Industrial and Corporate Change*, *24*(2), 307–343. https://doi.org/10.1093/ICC

Sidak, J. G., & Skog, J. O. (2015). Attack of the Shorting Bass: Does the Inter Partes Review Process Enable Petitioners to Earn Abnormal Returns. *UCLA L. Rev. Discourse*, *63*, 120.

Song, C., & Han, S. H. (2017). Stock Market Reaction to Corporate Crime: Evidence from South Korea. *Journal of Business Ethics*, *143*(2), 323–351. https://doi.org/10.1007/s10551-015-2717-y

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216–229. https://doi.org/10.1016/j.cose.2015.12.006

Wright, P. C., & Roy, G. (1999). Industrial espionage and competitive intelligence: one you do; one you do not. *Journal of Workplace Learning*, *11*(2), 53–59. https://doi.org/10.1108/13665629910260743

Wu, J. (2021). Database of Federal Cases. Retrieved from Federal Cases website: https://jeremy-wu.info/fed-cases/

Yang, D. (2019). Patent Litigation Strategy and Its Effects on the Firm. *International Journal of Management Reviews*, *21*(4), 427–446. https://doi.org/10.1111/ijmr.12202

Zeidan, M. J. (2013). Effects of Illegal Behavior on the Financial Performance of US Banking Institutions. *Journal of Business Ethics*, *112*(2), 313–324. https://doi.org/10.1007/s10551-012-1253-2

Zwillinger, M. J., & Genetski, C. S. (2000). Calculating Loss Under the Economic Espionage Act of 1996. *Geo. Mason L. Rev.*, *9*, 323.