Snatched Secrets: Reporting Trade Secrets Theft

Modelling a firm's decision to report a theft of trade secrets

Dr. Atin Basu Choudhary
Professor
Virginia Military Institute

Dr. Nicola Searle
EPSRC Digital Economy Fellow[1]
Goldsmiths, University of London

AUGUST 2017, DRAFT

Paper prepared for the
European Association of Law & Economics (EALE) 34th annual conference
14-16 September, 2017, London, United Kingdom

Key words: trade secrets, economic espionage, cybersecurity

Abstract: A growing priority for firms and governments is the protection of trade secrets against theft. Trade secrets, often stored and protected in digital formats, represent key intangible assets for firms and strategic assets for economies. Recent years has seen the expansion of trade secrets protection in both US and EU law, as governments seek to adapt policy to the changing and expanding threat of cybercrime. Here, we build on US FBI policy to model the interaction between a firm and a government protection agency. We consider the decision by the firm to adopt high or low security measures to protect their trade secrets, the decision to report an incident of theft, and the government protection agency's assignment of low or high priority to the case. We find that whether security breaches are made public or not can be the margin that determines whether firms will invest in high security. Our findings suggest that adjusting reporting requirements could be a policy measure to help address the growing threat of trade secret theft.

[1] Searle's participation is supported by ESPRC Grant EP/P005039/1, Economic Espionage and Cybercrime: Evidence and Strategy.

I. Introduction

Headline figures suggest that the theft of trade secrets[2] costs the world's economies between one and three per cent of GDP annually[3]. Due to their secret nature, the veracity of these estimates is difficult to confirm, but the overall picture is clear – firms and governments view trade secrets as important assets, and their theft poses an economic threat.

Prior to the digital era, trade secret theft involved thriller-worthy plots such as using airplanes to photograph competitor's factories. These days, the theft of trade secrets is facilitated by the predominance of the storing of trade secrets in digital files, and the reliance on cybersecurity for their protection. In the context of cybercrime, criminals may target, often unseen, the crown jewels of a firm's intellectual assets. Despite the economic impact of trade secrets and their theft, the relative paucity of data has lead to neglect by the research community (Arundel 2001, Almeling 2012, Morikawa 2014). We seek to address this gap in the literature.

This paper develops an economic model that details the interplay between firms, their choice of security measures, and the government security agencies tasked with protecting trade secrets and prosecuting their theft. The next section provides a summary of the relevant policy background, followed by a literature review; we then proceed to develop and analyze our model and its firm behavior and policy implications; our final section concludes and points to future areas of research.

II. Policy background: EU and US

The protection of commercial, intangible assets, known as trade secrets, against cyber espionage is a top priority for governments worldwide. In line with these priorities, the EU approved the Trade Secrets Directive in April 2016, which expands trade secrets protection. The 2015 draft of the EU Trade Secret Directive states the intention to improve legal protection of trade secrets to, "…enhance the competitiveness of European businesses and research bodies, which is based on trade secrets, and also improve the conditions/framework for the development and exploitation of innovation and for knowledge transfer … to improve the EU's competitiveness in the global knowledge economy."[4]

---

[2] A trade secret must meet the following criteria: 1) it must be secret, 2) it must have commercial value because of its secrecy and 3) it must be subject to reasonable steps to maintain its secrecy.[2] It differs from other forms of Intellectual Property (IP) protection, particularly patents, in that it does not require disclosure (being made public), does not expire and does not require registration. The relatively low threshold is balanced by its relatively low protection, as trade secrecy protection can be lost through independent discovery, reverse engineering, misappropriation[2], and theft. This paper focuses on the theft of trade secrets, it also covers the theft of trade secrets to benefit a foreign entity, which is commonly known as economic espionage.

3 Center for Responsible Enterprise and Trade, and PWC (2014) "Economic Impact of Trade Secret Theft," available at: http://www.pwc.com/us/en/forensic-services/publications/economic-impact.html. This estimate is calculated for the world's top 40 economies. The authors note the limitations of estimates of trade secret valuations, and use a combination of R&D spending and white collar crime as proxies for the annual theft of trade secrets.

[4] EU (2015) "Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure," Document 17392/13 + ADD 1 PI 18 CODEC 2842

Accompanying European policy debates is the expansion of trade secrecy protection in the United States. In May 2016, The Defend Trade Secrets Act was enacted, its summary states that "trade secret theft harms owner companies and their employees." This expansionist tendency of recent US and EU trade secrets policy may have unintended consequences. For example, expanded protection could aggravate censorship and transparency issues highlighted by trade secrets researchers (Turilli and Floridi 2009, Pasquale 2011, Levine 2014). Such a protectionist direction will also impact whistleblowing (Lindblom 2007, Khoury 2014) and limit employee mobility (Reder and O'Brien 2012, Png and Samilia 2013, Selmi 2014). Employee mobility, which should allow for the diffusion of innovation, also interacts with innovation policy; Png (2012) demonstrates the positive economic impact, notably in Silicon Valley, of Californian laws preventing employers from using trade secrets to limit their employees' ability to work for competitors. Thus, improved understanding of the interplay between key actors in trade secrets should provide insights into the theft of trade secrets and help optimize trade secrets policy.

FBI and the 'Fight' Against Theft

Modern policy has adopted a decidedly bellicose tone in protecting the economic role of trade secrets, with the American Federal Bureau of Investigation (FBI) particularly noted as having adopted a war narrative (Rowe, 2016) in treating the theft of trade secrets as a threat to national security. Dreyfuss and Lobel (2016) likewise note a strong US rhetoric where economic espionage is now treated as military espionage, and US firms as potential allies. This accompanies the increasing politicization of cybersecurity and complex interactions between actors (Basuchoudhary and Choucri, 2014.) In the US, FBI investigation of trade secret theft is done as part of a counterintelligence and white-collar crime remit. However, the policies put in place instead suggest that, in the face of limited resources, the FBI's policy preference is to encourage awareness higher protection of trade secrets by firms; this suggests a strategy of prevention, rather than prosecution, of theft. The Obama Administration's 2013 Strategy on Mitigation the Theft of U.S. Trade Secrets notes five strategic actions:

1. Focus Diplomatic Efforts to Protect Trade Secrets Overseas
2. Promote Voluntary Best Practices by Private Industry to Protect Trade Secrets
3. Enhance Domestic Law Enforcement Operations
4. Improve Domestic Legislation
5. Public Awareness and Stakeholder Outreach

The FBI further suggests the prioritization of the prosecution of well-protected, high-value trade secrets, as the reporting checklist[5] requires significant details on the value and protection measures. This paper will build on these preferences and policies, to develop a model of the interaction between government security agencies and firms.

III. Literature Review

The trade secrets and cybercrime literatures have largely developed independently. In this section, we detail the relevant literature and tie together the two strands.

[5] "Checklist for Reporting an Economic Espionage or Theft of Trade Secrets Offense" FBI (2017).

Trade Secrets as a means of appropriation

In both the US and EU policy debates, the emphasis is on the *economic* impact of trade secrets and the immediate need for their protection. Existing economics literature largely focuses on trade secrets as a means to provide a legal structure for innovators to appropriate the returns to their innovation. This literature falls under the economics of Industrial Organization and Innovation, with a strong emphasis on Intellectual Property aspects of trade secrets.

A key theme in the literature is to examine the firm's decision to use trade secrets. A core model is Anton and Yao (2004), which finds that, particularly when property rights are weak, firms use trade secrets to protect their 'big' innovations, and patents to protect 'little' innovations as disclosure outweighs the benefits of the relative strength of patents. Other authors also use models to investigate the decision between trade secrets and patents (Bhattacharya and Guriev, 2006; Bulut and Moschoni, 2006; Ottoz and Cugno, 2006, 2008; Kultti, Takalo, and Toikka, 2007; Mosel, 2011; Kwon, 2012; Panagopoulos and Park, 2015); or disclosure versus secrecy (Mukherjee and Stern, 2008). Generally, the literature frames the costs of protection of trade secrecy as a cheaper alternative to the costs of patenting. An exception is Henry and Ruiz-Aliseda (2016), who examine the dynamics between holders of a trade secret, the level of protection, competitors and efforts to "break" the trade secret through reverse engineering. The authors consider the cost of a protection (which could include cybersecurity) as an entry cost into trade secret ownership and note that this can serve as a barrier to entry.

Limited empirical evidence also suggests that trade secrets are a preferred measure of protection for innovations (Cohen et al 2000, Arundel 2001, Anton & Yao 2004, Png 2012, 2015; Crass et al, 2016). Hall et al (2014), provide a literature review of the empirical and theoretical literature on the subject. The literature has largely emphasized the role of trade secrets as a means of appropriation and competitive advantage.

Theft

While trade secrets as a means of appropriation are vulnerable to reverse engineering, the increasing policy and industry interest is on theft as a vulnerability. Largely committed in the cyberworld, the theft of trade secrets differs from more general interpretations of theft. Unlike tangible property, the theft[6] or misappropriation of IP, which is intangible, does not deprive the owner of the property. This nuance leads some scholars to challenge treating IP theft as a crime (Moore 2007). However, unlike other types of intellectual property, such as patents and copyright, the misappropriation of a trade secret undermines its very definition – it negates its secrecy. Thus, the owner is not deprived of the use of the trade secret, but of its secrecy and associated value. Similar dynamics in value and protection apply, to varying degrees, to other cybersecurity breaches classified by Gordon et al (2011) as breaches of: confidentiality (confidential information), availability (e.g. denial of service), and integrity (e.g. website defacements.)

[6] Theft or misappropriation is contrary to criminal or contract law and therefore illegal. This is distinct from independent discovery or reverse engineering, which are legal.

The empirical legal literature has begun to address the impact of theft of trade secrets. Carr and Gorman (2001) find that the announcement of the theft of trade secrets negatively impacts the stock market price of the trade secret owner, which is evidence of an incentive not to report; Cavusoglu et al (2004) have similar findings. Argento (2012) provides a legal analysis of the decision to report a theft. In particular, the author delves into reasons a firm may *not* report or pursue a trade secret theft. These are: failure to detect the misappropriation, inability to identify the perpetrator, embarrassment, concern about disclosing the trade secret, business diplomacy, and convenience. In particular, Argento notes, "a CSI/FBI survey found that 48 percent of respondents cited *negative publicity* as a reason for not reporting a computer security breach to law enforcement." [emphasis added] This approach is at odds with FBI efforts to improve the protection of trade secrets through criminal law; if trade secrets owners do not use existing tools, then the deterrent effect of the law is weakened.

Cybersecurity

In recent years, economists' interest in analysis of firm, hacker and government agency decision has increased. This literature falls under the realm of privacy breaches, software vulnerabilities and general hacks. Here we focus on those most relevant to our model. Png et al (2006) develop a theoretical model in which they note that an increase in enforcement (i.e. the government agency increasing its prosecution of hackers), could lead to a decrease in firm's protection measures and hence an increase in demand for enforcement. They describe the potential unsustainability of this approach and note instead, under certain conditions, and in keeping with the FBI's strategy, that promoting user protection measures is an efficient strategy. Gordon et al (2015b) acknowledge that limited empirical evidence exists to evaluate the effectiveness of existing policy encouraging firms to invest in their cybersecurity, but that government support for training and awareness may allow firms to better allocate their cybersecurity budget.

Further policy-related analysis can be found in Arora et al (2008); the authors examine factors affect the timing of the disclosure (report) of software vulnerability and the policy measures to optimize this. They argue that both immediate disclosure and secrecy (no disclosure) are suboptimal, firms generally report too late and that policy makers should encourage a relatively short period between discovery and disclosure. Romanosky et al (2011) find empirical evidence suggesting that policies requiring firm disclosure of data breaches have reduced the impact of breach-related crime. We discuss similar policy measures in our findings.

The cybersecurity literature generally includes IP theft but does not focus on it specifically. A notable exception is Andrijcic and Horowitz (2006), who develop a macroeconomic model to estimate the impact of cyber security risks on IP. The authors note that IP theft can have longer-term, insidious impacts on firms compared to short-lived cyber attacks such as denial of service. This suggests that IP theft represents an important strategic concern, in keeping with the policy concerns described in the introduction.

At the firm level, cyber attacks and theft pose a threat to performance. While the Carr and Gorman (2001) paper finds a negative stock market performance impact following the announcement of a trade secrets theft, and Andrijicic and Horowitz (2006) note that IP theft can have longer-lasting impacts, the impact of other types of

security breaches is inconsistent and may be surprisingly short-term or negligible. An empirical study by Aquisiti et al (2006) find that the negative stock market impact of data breaches (private customer data) is statistically significant but short-lived, but note that the indirect damage to trust and goodwill, and higher insurance premiums in the future may harm firm performance. Similarly, Davis et al (2009) find evidence that cyber security incidents such as data breaches do not impact web traffic for online businesses, and, as a result, they argue it is difficult for policy makers to encourage investment in cybersecurity. Hilary et al (2016), examining data breaches, argue, "the market reaction to cyber-breaches is statistically significant but economically limited."[7] More recent papers suggest that the impact may be changing. Gordon et al (2011) finds a significant, negative impact on stock market prices (particularly when the breach is affects availability), but that the impact appears to be deccreasing as investors lower the expected costs of such breaches. A recent paper by Arcuri et al (2017) suggests that the literature on the topic has mixed findings over the previous 20 years, and their research finds in favor of a negative, significant stock market reaction to announcements of information security breaches.

Collective security

A common theme in the literature is the argument that cybersecurity is a collective good with significant positive externalities and that, much like immunizations, investment in cybersecurity encourages 'herd immunity.' However, the economics of effecting the collective benefits are less straightforward with incentives often being suboptimal and numerous market failures, particularly given the need to focus on collaboration at the system, rather than individual, level (Andersen and Moore, 2006).

A number of authors examine coordination problems and make suggestions for policy solutions. Gordon et al (2015a) note private underinvestment by private actors is the default outcome as positive externalities are not included in decision-making, and argue in favour of government regulation to increase cyber security investment. Basuchoudhary and Choucri (2014) argue that, depending on the strength of international governance systems, cybersecurity can be akin to a stag hunt game, or, the authors note, a prisoners' dilemma where cooperation is costly. They argue that culture of computer users, in combination with the strength of governance systems, influences the optimal policy design. No clear solution has emerged.

Beckerian implications

There is an obvious overlap between the modelling of trade secrets theft and the Beckerian cost-based approached to crime. Adopting the basic Beckerian model, the theft of trade secrets has important implications on private prevention costs and loss, public expenditures on crime fighting and social loss. Becker (1968) details the industry of crime, of which cyber security expenditures, FBI investigations and the benefits to criminals of crime all play a part. He argues that social loss is a function of damages, costs of apprehension & conviction, the social cost of punishment and the number of offenses. Becker models fines as potentially social welfare increasing as they function as a form of transfer pricing, whereas incarceration, which is measured as a unit of time, can be more effective as a punishment as it can be a heavier resource burden on the criminal.[8] Empirically, there are challenges to calculating the relevant

[7] Hiliary et al (CITE), p. 4.

[8] The optimality conditions vary. Becker notes that the 'harm' caused by fines or incarceration should outweigh the gains to the criminal. Yet, in some cases, defendants with limited financial resources may

Beckerian utility and loss functions. The level of cybercrime is unknown, as crime is not always detected, and the value of the trade secrets is notoriously hard to predict.

The question for the theft of trade secrets is the optimal levels of private and public investment in detection and prevention of theft (cybersecurity), and the optimal level of investment in deterrence via the expected punishment (detection and punishment levels.) As Hua and Bapna (2003) describe, investment in cybersecurity reduces the losses to firms and note that that the literature generally focuses on the classic deterrence model in cybersecurity.

Our model focuses on two categories in the 1968 Beckerian model of crime, with the aim of providing insight into optimal public policy. The areas of our focus are: apprehension & conviction (public expenditures) and protection & apprehension (private expenditures.) We take as given the remaining three elements: damages, supplies of offenses and punishments. Additionally, we focus on the interplay between public policy objectives and firm behaviour, rather than total social loss to society. As outlined in the discussion on FBI strategy, one goal of current public policy is to reduce the social loss by encouraging private investment in protection (cybersecurity). The general expectation is that this is efficient both in terms of reducing the supply of offenses and damages, and, potentially, a more efficient balance of public versus private expenditures.

We assume that theft is given, and that the supply of offenses, damages and punishment are independent of the model. Within the two categories of interest, we examine private and public expenditures. Becker notes that cost (C) to apprehend & convict criminals is a function of activity (A), which is police and judicial activity. A itself is a function of manpower (m), resources (r) and capital (c). The FBI must gauge the correct C_{public} in order to achieve an efficient outcome. However, as Becker notes, echoed in Png et al (2006), private expenditures, by the individual in our case C_{firm}, are negatively related to both C_{public} and $C_{private}$ (the set of expenditures by other firms.) This is a problem in the face of the 'herd immunity' achieved by collective expenditure on cybersecurity. This misalignment between the incentives of the individual firm, total C and the overall social loss again supports the rationale behind the FBI's efforts to encourage private investment, although its ultimate efficacy remains to be seen.

IV. The Model

We model a signaling game with two players. The sender is a firm. This firm can be of two types. Type HS has a high security cyber environment. Type LS has a low security cyber environment. Nature chooses the type; the likelihood of a high security firm is P(HS) = α. Either type of firm can report an exogenous breach -- like stealing of a trade secret -- of their cybersecurity environment. They may also choose to not report a breach. This report signal is received by some government security agency. This agency has does not know whether the report is coming from a HS or LS type firm. However, the agency does have to decide whether to place a high or low priority

---

unable to pay ("judgment proof") and incarceration may be the only feasible punishment. Becker notes that the value of prison time will vary between defendants, and thus the 'fairness' of the punishment also varies.

on the report, in the interest of maintaining an efficient level of C_{public}. The agency has a Bayesian belief about the likelihood of receiving a report from a high security firm. This Bayesian belief drives the agency's likelihood of placing a high priority on following up on a report.

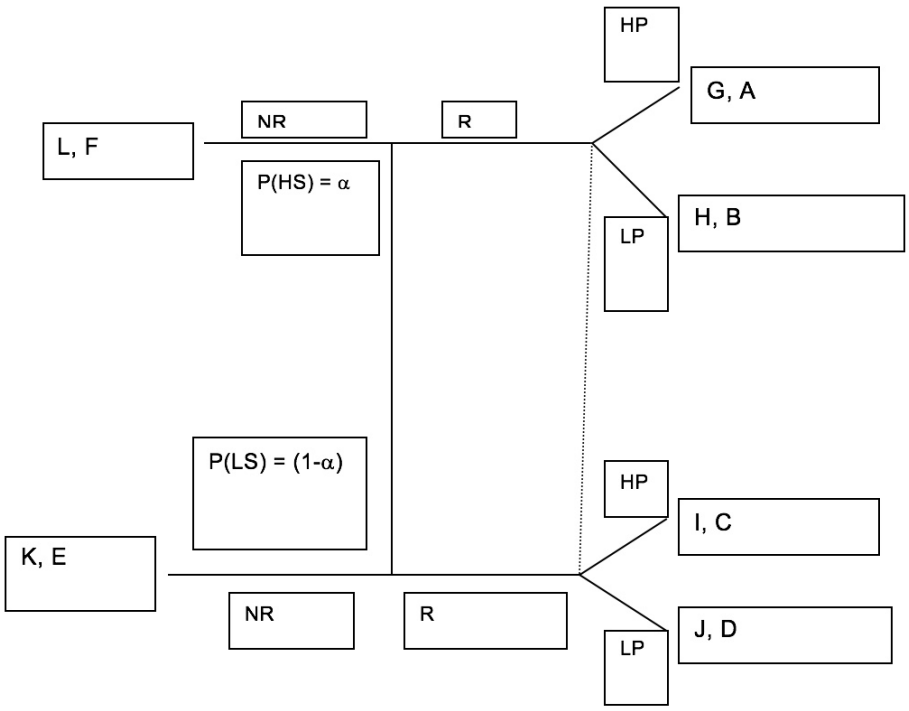

Figure 1. The Signaling Game

The players have preference ordering over actions. We model preference orderings under two conditions – when a security breach goes public and when it does not. Moreover, we assume that reporting a breach always makes the breach public. However, we model two circumstances if the firm does not report the breach. In one case the breach goes public whether the firm reports it or not. In another the breach only goes public if the firm reports it and not if it does not. In all these cases, we assume that the hacker is found and convicted automatically if the security agency places a high priority on a report and the firm is HS[9]. The payoff preference orderings for the two players are as follows.

The security agency's payoffs in order of preference are A > B > E > F > D > C. Thus, for example, the agency prefers to place high priority on reports from a high security firms rather than a high priority on a low security firm (A > C). In fact, it would prefer not receiving any report at all over receiving reports from a low security firm, as prosecutions in the face of low security are unsuccessful[10] (F and E are

[9] In Beckerian terms, the probability of conviction p = 1 if HS, HP, 0<p<1 if HS, LP and p = 0 if LS.
[10] In order to qualify for trade secret protection, the knowledge in question must be subject to reasonable steps of protection; low security is assumed not to have met, ex post, this threshold. Anson

preferred over C and D). Nevertheless, it would rather not receive a report from a low security firm than a high security firm (E > F). In any case the agency would rather place a high priority rather than a low priority on reports it believes are coming from high security firms (A > B) and vice versa if it believes reports are coming from low security firms (D > C). The security agency does not care whether a security breach goes public or not.

If a security breach goes public irrespective of whether a firm reports it or not the payoff preference ordering is G > H > I > J > L > K. Thus, a high security firm having done due diligence on security would rather have the security agency place a high priority on their report than a low priority and in any case, would rather report than not report (G > H > L) since in any case there is no advantage from hiding the breach. In fact, the low security firm would also prefer reporting to not reporting in order to avoid bad publicity and the liability cost of not reporting given the assumption that the breach is bound to go public (I and J are both > K). We further assume that L > K because even if the breach goes public the high security firm can at least claim to have tried to deter criminals by securing their network and therefore avoid the sort of liability faced by low security firms that did not even try to do the right thing.

On the other hand, if the security breach does not go public then the payoff preference ordering is G > L > H > K > I > J. First of all, the lack of publicity changes the low security firm's payoffs and skews it toward not reporting at all since the liability from going public no longer exists. Nevertheless, if the low security firm did report it would prefer that the security agency place a high priority on the report. This is moot though since the low security firm will never report under the circumstances. The high security firm though is faced with a conundrum. If it reports the breach to the security agency then, as always, it prefers a high priority by the security agency. The security agency's use of high priority will result in conviction of the perpetrators IF HS, minimise the ability of competitors to use the innovation protected by the trade secret and may result in criminal damages[11] paid to the firm. However, the firm would rather not report if it believes that the report will receive a low priority from the security agency. Recall reporting leads to public revelation of the breach. A low priority by the security agency then would not only *not* result in a conviction but it would reveal that the breach happened and tarnish the firm's reputation.

V. Model Analysis and Results

As noted above our model has two cases – one where a security breach goes public irrespective of whether a firm reports it to the security agency or not and another where the breach is only made public if the firm reports the breach. We analyze each case below.

---

and Suchy (2005) note that trade secrecy protection is often only determined when conflict has arisen (similar arguments exist for patents, in which the validity and scope of a patent may only be defined through litigation.)

[11] To note that damages here mean damage payments. Under Becker's (1968) model, damage payments mean that most punishments can produce a gain for the victim. Here, we question that assumption as the negative impact on the firm's reputation (in a repeated game) may outweigh any financial gain from transfer payments (damage payments.)

Case 1. The security breach goes public. In this case, the high security firm prefers G and H over L. The low security firm also prefers I and J over K. Both types of firm's then will always report to the security agency. The security agency knows that in this pooling scenario it is likely to get a report from a HS firm with α probability. Thus, it gets a report from a low security firm with probability 1 - α. The security agency then calculates its expected payoffs from placing a high priority and compares it to its expected payoffs from placing a high priority. It then chooses the strategy with the higher expected payoff. The expected payoffs are:

$$E(HP) = \alpha A + (1 - \alpha)D \quad (1)$$

and

$$E(LP) = \alpha B + (1 - \alpha)D \quad (2).$$

Thus, the security agency will only place a high priority on a report iff (1) > (2) i.e. if

$$\alpha > (D - C)/(D - C + A - B) \quad (3).$$

Notice that (3) is certainly plausible since it requires that α be greater than some positive fraction.[12] Thus, our result suggests that the security agency will place a high priority on a report only if the likelihood of a HS type firm is high and will *place a low priority on any report otherwise*. From a policy perspective then the fact that all breaches go public does counterintuitively create a space where the security agency is unlikely to place a high priority on any report! One possible dynamic effect of such a situation could disincentivize firms from choosing high security in the first place and further depressing α.[13] This could create a vicious cycle where firms do not choose high security at all – after all why bother if the security agency is unlikely to pay attention and do something about it. Under these circumstances the only possible stable option may be to force the security agency to always give high priority to a breach or hack as a matter of enforceable law. Given that security agencies routinely prioritize law enforcement this seems unlikely. Another possible policy response may be to force firms to reveal their type on pain of punishment given the incentive structure where all security breaches ultimately go public. The FBI reporting checklist requires significant disclosure on protection measures, which may be an indication that some form of triage already exists.

Case 2. The security breach does not go public if unreported. In this case notice that the firm's payoff structure suggests that the LS type firm will never report a security breach. The HS type firm though will report a security breach if it believes that the report will be accorded a high priority but not otherwise. This creates a scenario where both types of firm's may not pool (always report) on reporting a breach. This opens the possibility of a mixed strategy Bayesian Nash Equilibrium. However, the truth is simpler. In this case, the fact that the LS firm will never report a breach means that all reports MUST be from the HS firm even if some HS firms choose not to report. Thus, from the security agency's perspective the likelihood that a reported

[12] (3) is always a positive fraction since the denominator will always be larger than the numerator and positive given the rank ordering of the payoffs.
[13] We do not model this endogeneity here but it seems like a plausible inference.

breach is from a HS type is 1. Given this belief is optimal for the security agency to always place a high priority on any reported breach. Of course, in that case the HS type firm should always report. In other words, when not reporting a breach never becomes public, then the HS firm always reports, the LS firm never reports, and the security agency always places a high priority on a reported breach. This, of course is ideal from the security agency's perspective. In fact, though we do not model α endogenously in this paper, over time this scenario may encourage firms to choose high security.

Policy implications

The key objective of the US government, as demonstrated by FBI policy, is to reduce the level and impact of trade secret theft. In the face of limited resources and relatively unlimited demands, it is FBI policy to encourage improved security at the firm level. As we have noted, existing FBI policy is generally soft encouragement through awareness and training measures. However, as our model has shown, the threat of a theft going public may be sufficient incentive for a firm to choose HS. At HS, the firm is in a good position even if they are in Case 2, as they still report. For firms who have chosen LS, the threat of going public is a sufficient disincentive that it provides a policy lever for the FBI. A number of solutions present themselves to encourage disclosure: theft reporting requirements, financial reporting requirements and data breach reporting requirements. However, it may ultimately be that the role of encouraging investment in cybersecurity inadvertently falls to the courts.

In theft reporting, the FBI could adopt a harder measure in requiring the disclosure, such as a mandatory reporting law. In this scenario, a victim firm would be required to report the theft of the trade secret – providing a strong incentive, based on the potential costs of bad publicity, to have prevented the theft in the first place through HS. Currently, under the US Law Failure to Report a Crime under Federal Law (18 U.S.C. section 4, also known as misprision of a felony), only active concealment, rather than failure to report, is against the law (e.g. only following direct question during a federal investigation would the firm (employees) be required to report.) However, the introduction of broader requirement to report would have to be delicately worded with a very narrow scope so as not to discourage the use of trade secrets in the first place, in addition to unintended consequences such as implications on whistle-blowers and journalists. Such a solution may also present civil liberty concerns.

Building on existing financial reporting regulations, such as the reporting requirements of listed companies, could also encourage good practice by firms. Currently the annual 10-K form includes a section on speculation and risk, where cybersecurity breaches can be reported. Hilary et al (2016) find that the use of this section has increased modestly [14] over the period 2010-2015. Additionally, cybersecurity levels, measured by spend and incidents, could become part of standard reporting requirements. Likewise, where firms have chosen to include valuations of IP on their balance sheets, the loss of secrecy through theft would also imply the need to

[14] The authors find that the proportion of firms using this section increased by 11% in their sample of 147 firms that had suffered a data breach, and by 17% in the control group.

adjust the balance sheet accordingly. Insurers may also play a role in this, as trade secrets can be insured and policies likely require reporting when secrecy is impacted.

Further possibilities existing under data protection laws. The protection of personal data, which could ostensibly be covered by trade secrecy, may be covered by existing privacy protection laws. In the event of a cybersecurity breach resulting in the theft of such data, firms would be obligated to disclose the theft. Similar disclosure policies in data breaches are estimated to reduce identity theft by 6% (Romanosky et al, 2008) and increase investment in cybersecurity (Hoofnagle, 2007). Yet Hilary et al (2016), find that US policies to encourage disclosure have lead to only a modest increase in disclosures. However, disclosure requirements may provide an additional incentive to invest in cybersecurity, in an attempt to avoid bad publicity, yet could result in over-reporting and negatively impact FBI resources. Additionally, such regulations will increase costs to businesses.

A related option, and one that is likely the most probable in the foreseeable future, is that the courts will refine what counts as "reasonable protection" in order to qualify for trade secrecy. This is akin to decisions in other areas of IP, such as setting the level of inventiveness in patents or the delineation of infringement in copyright – both of which are established policy levers. If the bar is set higher than current levels of protection, then firms will be incentivized to invest in cybersecurity in order to protect their trade secrets. This could achieve the FBI's goal to encourage investment and reduce theft, without the concerns about reporting and potential strains on FBI resource. However, this approach could go both ways – courts may either raise or lower the security bar, as decisions are based on individual cases. The court need not consider the wider 'herd-immunization' implications, which could result in the bar being set below the socially efficient level.

Finally, Becker's analysis becomes relevant again here. While we have focused on the FBI's desires to reduce theft via increased private investment cybersecurity ($C_{private}$), Becker also notes that the expected utility of crime (EU), which is a function of the probability of prosecution (p), punishment (f), and the income from the crime (Y) also influence the supply of crime. While $C_{private}$ increases p by increasing the probability of detection, it is beyond direct FBI control. However, the FBI could choose direct action to reduce EU by increasing p through increasing C_{public} or increasing f through legislation (in conjunction with government.) These classic Beckerian policy options merit further exploration and reflect the increased criminalization of trade secret theft.

VI. Conclusion

In this paper, we model a scenario where a cybersecurity breach could affect firms who may have high security or low security. Security agencies in their turn may not know if a firm is a high or a low security firm. They would like to prioritize reports from high security firms and convict hackers. We find that when unreported breaches inevitably become public the security agency might (if α is low enough) choose to never place a high priority on any report. This sort of scenario may generate a vicious cycle where more and more firms choose to go with low security given that the security agency does not investigate cyber-attacks because it believes that reports are more likely to come from low security firms. This effect is eliminated if not reporting a security breach guarantees the privacy of the firm. In this case, the low security firm

never reports a security breach while the high security firm always reports a breach and the security agency places a high priority on all reports because it believes them to be from high security firms. This separating equilibrium may then jumpstart a virtuous selection process encouraging more firms to adopt high security. Thus, publicity may paradoxically enhance the likelihood of adverse selection and worsen the security environment in cyber space.

Our model presents a number of extensions and possibilities for future research. In particular, we have assumed that the firm knows ex ante whether their theft will go public. Removal of this assumption could change the outcomes significantly, as the negative publicity from not reporting a theft could shift the firm's preferences. Additionally, incorporation of the policy measures we have suggested could manipulate outcomes in favor of FBI preferences. We have necessarily focused on a single-firm case, however a more macro approach could provide insights into welfare impacts, firm interactions and international implications. There is also some room for empirical exploration of our theory; differences between jurisdictional approaches to data breaches and trade secret theft may provide room for natural experiments to test our policy conclusions. As cybercrime and trade secrets continue to be a growing concern for firms and governments, we expect to see increased research interest in this area.

VII. References

Acquisti, Alessandro, Allan Friedman, and Rahul Telang. "Is there a cost to privacy breaches? An event study." *Proceedings of the Twenty-Seventh International Conference on Information Systems (citeseerx. ist. psu. edu/viewdoc/download? doi= 10.1. 1.73. 2942&rep= rep1&type= pdf*. 2006.

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

Anderson, Ross, and Tyler Moore. "The economics of information security." *Science* 314.5799 (2006): 610-613.

Andrijcic, Eva, and Barry Horowitz. "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property." *Risk analysis* 26.4 (2006): 907-923.

Anson, Weston and Donna Suchy, Editors, (2005),Fundamentals of Intellectual Property Valuation, The American Bar Association, Chicago, Illinois.

Anton, J. J. & Yao, D. A. (2004) Little patents and big secrets. *RAND Journal of Economics*, 1-22.

Arcuri, Maria Cristina, Marina Brogi, and Gino Gandolfi. "How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns." ITASEC. 2017.

Argento, Zoe. "Killing the Golden Goose." *Yale Journal of Law and Technology* 16.1 (2015): 5.

Basuchoudhary, Atin, and Nazli Choucri. "The evolution of network based cybersecurity norms: An analytical narrative." Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on. IEEE, 2014.

Bhattacharya, Sudipto, and Sergei Guriev. "Patents vs. trade secrets: Knowledge licensing and spillover." *Journal of the European Economic Association* 4.6 (2006): 1112-1147.

Bulut, Harun, and GianCarlo Moschini. "Patents, trade secrets and the correlation among R&D projects." *Economics Letters* 91.1 (2006): 131-137.

Carr, C. & Gorman, L. R. (2001) The revictimization of companies by the stock market who report trade secret theft under the Economic Espionage Act. *Business Lawyer*, 57(1).

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers." *International Journal of Electronic Commerce* 9.1 (2004): 70-104.

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

Crass, Dirk, et al. "Protecting innovation through patents and trade secrets: Determinants and performance impacts for firms with a single innovation." (2016).

Cugno, Franco, and Elisabetta Ottoz. "Trade secret vs. broad patent: The role of licensing." *Review of law and economics* 2.2 (2006): 209-21.

Davis, Ginger, Alfredo Garcia, and Weide Zhang. "Empirical analysis of the effects of cyber security incidents." *Risk analysis* 29.9 (2009): 1304-1316.

Dreyfuss, Rochelle Cooper, and Orly Lobel. "Economic espionage as reality or rhetoric: Equating trade secrecy with national security." *Lewis & Clark L. Rev*. 20 (2016): 419.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. "Externalities and the magnitude of cyber security underinvestment by private sector

firms: a modification of the Gordon-Loeb model." Journal of Information Security 6, no. 1 (2015a): 24.
Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Lei Zhou. "Increasing cybersecurity investments in private sector firms." Journal of Cybersecurity 1, no. 1 (2015b): 3-17.
Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. "The impact of information security breaches: Has there been a downward shift in costs?." Journal of Computer Security 19.1 (2011): 33-56.
Hall, Bronwyn, et al. "The choice between formal and informal intellectual property: a review." *Journal of Economic Literature* 52.2 (2014): 375-423.
Hilary, Gilles and Segal, Benjamin and Zhang, May H., Cyber-Risk Disclosure: Who Cares? (October 14, 2016). Georgetown McDonough School of Business Research Paper No. 2852519. Available at SSRN: https://ssrn.com/abstract=2852519 or http://dx.doi.org/10.2139/ssrn.2852519
Hoofnagle, C. J. (2007). Security breach notification laws: Views from Chief Security Officers.
Kultti, Klaus, Tuomas Takalo, and Juuso Toikka. "Secrecy versus patenting." *The Rand journal of economics* 38.1 (2007): 22-42.
Kwon, Illoong. "Patent races with secrecy." *The Journal of Industrial Economics* 60.3 (2012): 499-516.
Lemley, M. A. (2015) Faith-Based Intellectual Property. *UCLA L. Rev.*, 62, 1328.
Lindblom, L. (2007) Dissolving the moral dilemma of whistleblowing. *J. of Bus. Ethics*, 76(4), 413-426.
McGowan, M. K., Stephens, P. & Gruber, D. (2007) An exploration of the ideologies of software intellectual property: The impact on ethical decision making. *Journal of business ethics*, 73(4), 409-424.
Moore, A. P., D. M. Cappelli, T. C. Caron, E. Shaw, D. Spooner, and R. F. Trzeciak. *A preliminary model of insider theft of intellectual property*. No. MU/SEI-2011-TN-013.
Morikawa, M. (2014) Innovation in the Service Sector and the Role of Patents and Trade Secrets.
Mosel, Malte. *Big patents, small secrets: how firms protect inventions when R&D outcome is heterogeneous*. No. 105. BGPE Discussion Paper, 2011.
Mukherjee, Arijit, and Scott Stern. "Disclosure or secrecy? The dynamics of open science." *International Journal of Industrial Organization* 27.3 (2009): 449-462.
Ottoz, Elisabetta, and Franco Cugno. "Patent–secret mix in complex product firms." *American Law and Economics Review* 10.1 (2008): 142-158.
Panagopoulos, Andreas, and In-Uck Park. *Patenting vs. secrecy for startups and the trade of patents as negotiating assets*. mimeo, University of Crete, 2015.
Png, I. & Samila, S. (2013) Trade secrets law and engineer/scientist mobility. *WP Nat. U. Singapore*.
Png, Ivan PL. "Law and innovation: evidence from state trade secrets laws." Review of Economics and statistics 0 (2012).
Png, Ivan, Candy Q. Tang, and Qiu-Hong Wang. "Information security: User precautions and hacker targeting." *National University of Singapore* (2006).
Reder, M. E. & O'Brien, C. N. (2011) Managing the Risk of Trade Secret Loss Due to Job Mobility in an Innovation Economy with the Theory of Inevitable Disclosure. *J. High Tech. L.*, 12, 373.
Reichman, J. H. (2011) How trade secrecy law generates a natural semicommons of innovative know-how.

Romanosky, Sasha, Rahul Telang, and Alessandro Acquisti. "Do data breach disclosure laws reduce identity theft?." *Journal of Policy Analysis and Management* 30.2 (2011): 256-286.

Rowe, Elizabeth A. "RATs, TRAPs, and Trade Secrets." *BCL Rev*. 57 (2016): 381.

Selmi, M. (2014) Trending and the Restatement of Employment Law's Provisions on Employee Mobility. *Cornell L. Rev*., 100, 1369.

Stahl, B. C., Eden, G., Jirotka, M. & Coeckelbergh, M. (2014) From Computer Ethics to Responsible Research and Innovation in ICT. *Information & Management*, 51(6), 810-818.

Romanosky, S., R. Telang, and A. Acquisti (2008). Do data breach disclosure laws reduce identity theft? In Seventh Workshop on the Economics of Information Security - WEIS 2008

Tene, O. & Polonetsky, J. (2012) Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop*., 11, xxvii.

Turilli, M. & Floridi, L. (2009) The ethics of information transparency. *Ethics and Information Technology*, 11(2), 105-112.

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