Computers & Security 87 (2019) 101591

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Snatched secrets: Cybercrime and trade secrets modelling a firm's decision to report a theft of trade secrets ☆

Atin Basuchoudhary [a], Nicola Searle [b,*]

[a] Virginia Military Institute, Lexington, VA 24450 USA
[b] Goldsmiths, University of London, London, SE14 6NW, UK

ARTICLE INFO

Article history:
Received 10 March 2019
Revised 17 July 2019
Accepted 8 August 2019
Available online 8 August 2019

Keywords:
Cyber security
Cybercrime
Trade secrets
Economic espionage
Cyber breaches

ABSTRACT

Cybercrime and economic espionage are increasing problems for firms. We build on US FBI policy to frame the interaction between a cybercrime victim firm and a government security agency. We bring together several strands in the literature to model the strategies of the firm, which has suffered a cyber breach and theft of trade secrets, and the government security agency, which must investigate and prosecute crimes. We investigate the interactions between these two players, in which the firm has private information about its cybersecurity investment. This investment level is unknown to the security agency, which must nonetheless decide how to prioritize reported crime. We model this asymmetric information problem within a game theoretic signaling framework derived from Becker's work in crime and punishment. We suggest that such a framework can inform policy to encourage security investments by firms and more efficient resource utilization by security agencies. We particularly focus on an illustrative stylized example to highlight how our modelling approach can be helpful. In this example we compare two worlds; one where all security breaches become public knowledge and another where only reported breaches become public knowledge. We then formulate two potentially testable Hypotheses and several implications of these Hypotheses. Case studies and a policy analysis further highlight how our framework plays out in reality.

1. Introduction

For more than a decade, malicious actors have conducted cyber intrusions into United States commercial networks, targeting confidential business information held by American firms. Malicious cyber actors from other nations have stolen troves of trade secrets, technical data, and sensitive proprietary internal communications (Government of the United States, 2018).

Headline figures suggest that the theft of trade secrets[1] costs the world's economies between one and three per cent of GDP annually.[2] Unseen in the cyber world, criminals may target the crown jewels of a firm's intellectual assets. Firms and governments increasingly view trade secrets as important assets and cyber security as a key component of protection. However, researchers and practitioners alike do not have a clear understanding of the interrelated decision making process that determines whether firms report a theft, how government agencies assign resources in responding to a report, and how firms determine investments in private protection. There appears to be no analytical framework to address the interplay between firms, cyber security,[3] and the government security agencies tasked with protecting trade secrets and prosecuting their theft. We seek to address this gap in this paper. First, we discuss the literature that brings together different investigative concerns to connect the economic roles of trade

☆ Searle's participation is supported by the Engineering & Physical Science Research Council (EPSRC) Grant EP/P005039/1, Economic Espionage and Cybercrime: Evidence and Strategy.

* Corresponding author.
E-mail address: n.searle@gold.ac.uk (N. Searle).

[1] A trade secret, which is a type of intellectual property, 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. This paper focuses on two criminal aspects of trade secret misappropriation — the theft of trade secrets, and the theft of trade secrets to benefit a foreign entity, commonly known as economic espionage.

[2] The Center for Responsible Enterprise and Trade (CREATe.org) 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 calculated for top 40 economies using a combination of R&D spending and white collar crime as proxies.

[3] We use 'cybersecurity' as a term used to complement 'cybercrime'; 'information security' is another option to describe security for information assets (Von Solms and Van Niekerk, 2013).

https://doi.org/10.1016/j.cose.2019.101591

secret theft, cyber security and cybercrime. Second, we develop a conceptual framework which adapt the economics of crime to cybercrime and trade secrets theft, and explore this framework via a game theoretic model to capture complex contextual realities.

The next section provides 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.

2. Prior literature

Academic analysis has addressed the economic roles of trade secret theft, cyber security and cybercrime as separate themes, but crossover is relatively recent. In this section, we bring together four research strands relevant to our paper.

2.1. Vulnerable assets

The same technologies that have been a catalyst to the economic growth of both businesses and economies have created a new and threatening environment for the protection of vital assets. These new technologies make it easier to store, access, disseminate, and publish confidential information, thereby enhancing the likelihood that a trade secret may be lost (Goverment of the United States, 2013).

Trade secrets theft and cybercrime are closely related. While digital technologies have led to a boon for innovation and information management, intangible assets have simultaneously become more vulnerable. Digital assets include core value assets (e.g., intellectual property [IP], data, customer records, security information), and operational assets (e.g., business critical IT services) (Ruan, 2017). Trade secrecy can protect core value assets: trade secrets law helps address vulnerabilities[4] by providing legal protection for these digital assets; cyber security provides business critical, practical protection.

Governments are reacting to these challenges. The US government describes growing threats, "[competitors and adversaries are] engaging in pernicious economic espionage and malicious cyber activities, causing significant economic disruption and harm…" (Government of the United States, 2018: 1). In parallel to cyber policies, the US has sought to bolster legal support of trade secrets. Recent trade secrets debates have had a 'war narrative' (Rowe, 2016) in treating theft of trade secrets as a national security threat and US firms as potential allies (Dreyfuss and Lobel, 2016).

A firm's use of trade secrets is a strategic decision. In order to maintain a competitive advantage and protect innovations, firms must consider IP mechanisms to control use of their knowledge. Trade secrets, unlike other IP, do not require a formal registration process, potentially last forever, protect a broad class of information, and do not require disclosure. The wide scope of trade secrets means that firms can protect assets from customer lists to prototypes. Even failures, such as software vulnerabilities and unsuccessful scientific trials, qualify as trade secrets. A disadvantage of using trade secrets as a protection mechanism is that their *secrecy* is fundamental for their use; once made public, the trade secret is no longer a trade secret both in practical and legal terms. Good cyber security and legal controls such as contracts mitigate the risk of theft.

Firms have alternatives to trade secrets as legal and strategic mechanisms. In lieu of trade secrets, firms may choose to patent (e.g., Bhattacharya and Guriev, 2006; Bulut and Moschini, 2006; Cugno and Ottoz, 2006; Ottoz and Cugno, 2007; Kultti et al., 2007; Mosel, 2011; Kwon, 2012; Panagopoulos and Park, 2015). However, patents may provide shorter-term and expensive protection, and also involve making more information public, which can lead to the loss of a competitive advantage. Trade secrets can be a superior IP protection mechanism; limited empirical evidence suggests that trade secrets are preferred over other types of IP (*see* Cohen et al., 2000; Arundel, 2001; Anton and Yao 2004; Png et al., 2006; Crass et al., 2016; Png and Samila 2013; Png 2017a, 2017b).[5] Cyber security plays a small role in other IP, such as the use of technical protection measures to control copyrighted material, but is fundamental to the protection of trade secrets.

2.2. Costs and impact

Trade secret theft is costly to the firm; to mitigate or prevent thefts, the firm must invest in cyber security. Weighing the risks, costs, and benefits of cyber security and trade secrecy is important for firm decision-making and for academic analysis. Yet quantifying these elements is not straightforward.

For the legal protection of core value assets, trade secrecy is a lower cost approach than other IP.[6] However, it is unclear whether this remains true in the era of cybercrime as, in order to qualify for trade secrecy, the trade secret must be subject to a threshold of 'reasonable protection'. What qualifies as reasonable at one point may quickly become outdated as technology moves on Cash (2015). Effective cyber security may need frequent investments. 'Loss of confidential data' is a central risk included in security decision making (Moore et al., 2015). The classic Gordon and Loeb (2002) model argues that security investments exhibit decreasing marginal returns and limited security investment is justified for very low or very high vulnerabilities. In cases of widely known information, such as the possible sale of a business unit, the costs to protect information can be prohibitively expense. As a implication, the authors argue that the focus should not be on the vulnerability of the asset, but "the reduction in expected loss with the investment." Gordon and Loeb (2002, p. 450.)

Appraising the correct level of protection is difficult. Gordon and Loeb (2002) find the optimal investment in information security is less than or equal to 37% of the expected loss of unprotected assets. Lagazio et al. (2014) suggest that firms in the financial sector invest approximately one-to-two percent of their IT budget in security. Investment is increasing (Moore et al. 2015). A 2016 industry estimate finds firms spend 5.6% of their IT budget on security and risk management (McMillan and Olyaei, 2016). The intangibility and uncertainty of protection thwarts valuing the returns to investment in security and the expected loss of a trade secrets theft. Informed risk-assessment for firms is compromised by insufficient quantitative information (Ruan, 2017). Compounded by fast-changing technologies and cyberthreats, optimizing security investment levels remains a challenge.

Cybercrime can be costly to the firm. Data loss (the loss of confidential data and trade secrets) is a key business cost following a successful attack (Wei et al., 2005). Data loss reduces competitiveness due to compromised IP becoming available to competitors (Gordon and Loeb, 2002; Anderson et al., 2013; and Lagazio et al., 2014). IP theft can have *longer-term, insidious* impacts on firms compared to short-lived cyber attacks such as denial of service (Andrijcic and Horowitz, 2006). This suggests that IP theft represents an important strategic concern for the firm, in keeping with policy concerns described earlier.

[4] Trade secrets as a means of appropriation are also vulnerable to reverse engineering and independent discovery. This paper focuses on theft as vulnerability.

[5] See Hall et al. (2014) for a literature review of theoretical and empirical trade secrets research.

[6] Not all core value assets can be covered by other types of IP; trade secrecy covers a broader scope. Copyright is another low cost option but has a narrower scope than trade secrets.

There is limited empirical evidence of expected losses, despite the threats posed. The announcement of the theft of trade secrets or internet security breach negatively impacts a firm's stock market price (Carr and Gorman, 2001; Cavusoglu et al., 2004). While Carr and Gorman (2001) and Andrijcic and Horowitz (2006) note the negative impact of IP theft on firm performance, the impact of other types of security breaches is inconsistent and sometimes surprisingly short-term or negligible. Acquisti et al. (2006) find that the negative stock market impact of data breaches is statistically significant but short-lived, but note that the indirect damage to goodwill, and higher insurance premiums 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 argue it is therefore difficult for policy makers to encourage investment in cyber security. The impact may be changing. Gordon et al. (2011) find a significant, negative impact on stock market prices, but that impact decreases as investors lower the expected costs of such breaches. Hilary et al. (2016) argue that, "the market reaction to cyber-breaches is statistically significant but economically limited."[7] Arcuri et al. (2017) note that literature on the topic has mixed findings over the previous 20 years, and find in favor of a negative, significant stock market reaction to announcements of information security breaches. Collectively, the body of research describes a shifting landscape in which firms face uncertainty in estimating the impact of crime.

While both the theoretical and empirical literature demonstrate the negative impacts of cyber security threats and cybercrime, the decision-making for investments remains difficult. A firm's choice of investing in a high or low security environment is poorly understood and even the impact of a cyber breach or trade secret loss is ambiguous.

2.3. Government policy and cyber security

In policy debates, the emphasis is on the economic impact of cybercrime, trade secrets, and the immediate need for better cyber security. Yet interactions between actors are complex in cyber security (Basuchoudhary and Choucri, 2014). Cyber security is a collective good increasing social welfare with significant positive externalities and, like immunizations, investment in cyber security encourages 'herd immunity'. A firm's investment in cyber security has positive externalities and contributes to the wider ecosystem and security of trade secrets; investment also raises funds for software development and increases innovation in the economy (Cash, 2015). However, aligning the incentives of firms and governments is challenging.

Despite the need to focus on collaboration at the system level, rather than the individual level (Andersen and Moore, 2006) cyber security policies and investments are inefficient (Gordon et al., 2015a). For example, Png et al. (2006) argue that an increase in enforcement, leads to a decrease in a firm's protection measures and an increase in demand for enforcement. A policy solution could be government support for training and awareness, which may allow firms to better allocate their cyber security budget (Gordon et al., 2015b). Yet other authors suggest focusing on the user (Png et al., 2006, Basuchoudhary and Choucri, 2014) rather than on the firm. As policy often lags behind technology, and technology in this space is very fast-moving, any policy gains may be short-lived. This paper examines a government security agency's[8] decision-making in cybercrime as a policy lever to encourage investment in cyber security.

[7] Hilary et al. (2016), p 4.

[8] The FBI, for example, plays an important role in effecting these policies as a primary investigative agency for cybercrimes and is the agency responsible for federal investigations of economic espionage.

2.4. Government policy, investigations and reporting

Policy is being developed in a vacuum. Government policy is shaped by disclosed thefts, not those which go unreported (Lagazio et al., 2014). The Cyber Strategy (Government of the United States, 2018, p. 11) acknowledges this, "The prompt reporting of cyber incidents to the Federal Government is essential to an effective response, linking related incidents, identification of the perpetrators, and prevention of future incidents." Effective government policy is one that addresses the coordination problems associated with disclosure in order to move toward to a socially optimal equilibrium. Empirical evidence finds government policies requiring firm disclosure of data breaches have reduced the impact of breach-related crime (Romanosky et al., 2011).

While reporting is key to developing good policy and security, the incidence of reporting in practice is generally sub-optimal. Firms face risks both in disclosing a trade secret theft (further loss of competitive advantage, loss of goodwill, and potential loss of trade secrecy) and not disclosing the theft (ethical and legal implications, establishing a precedent of no implications for theft, and forgoing potential damages.) Argento (2013, p. 216) notes, "a CSI/FBI survey found that 48% of respondents cited negative publicity as a reason for not reporting a computer security breach to law enforcement." Firms are also reluctant to admit significant financial losses associated with cyber breaches (Shackelford, 2016). "The harm of the disclosure, both through publicizing internal vulnerabilities and reputational damage, can be worse that the initial attack."(interviewee, Ettredge et al., 2018, p. 568) Curiously, firms who disclose the existence of their trade secrets in their financial filings have a higher probability of subsequent cyber security breaches than firms who do not (Ettredge et al. 2018).

Yet disclosure, or not, can serve self-interests. Actors have incentives to over or under-report cybercrime (Moore et al., 2009; Anderson et al. 2013). For example, firms specializing in cyber security may over-report their successes (Gordon and Loeb, 2002) while governments may seek to minimize crime statistics; these competing incentives can lead to suboptimal outcomes. However, in a repeated game, not disclosing and, as a consequence, not pursuing criminal or civil redress can incentivize crime. This is at odds with FBI efforts to improve the protection of trade secrets through criminal law; if firms do not use existing tools, then the deterrent effect of the law is weakened.

The dynamics between firms and government enforcement agencies (e.g. the FBI), can create an 'under-reporting loop.' Using a systems dynamic causal (SDC) approach, Lagazio et al. (2014) model how victim firms chronically under-report causing the government to underestimate the extent of cybercrime, which reduces the effectiveness of cybercrime policing and ultimately leads to a growth in cybercrime incidents. Lagazio et al. (2014) link this loop to the firm's compromised IP and loss of trade secrets, leading to competitive disadvantages, and reputational damage. Our framework focuses on these relationships and the government's efforts to encourage reporting and investment in cyber security. This 'under-reporting loop' and some related nodes, summarized in Fig. 1, is the policy and crime context in which our analysis sits.

The question, combining the investigative strands described above, then remains – how does a security agency's decisions to investigate a crime interact with a firm's decision to report the crime and its decision to invest in more security?

In the following section we develop our conceptual framework by structuring this interplay between the government and the victim of a cybercrime. We then use this framework to answer the question above by comparing two scenarios: one where all breaches go public and one where only reported breaches go pub-

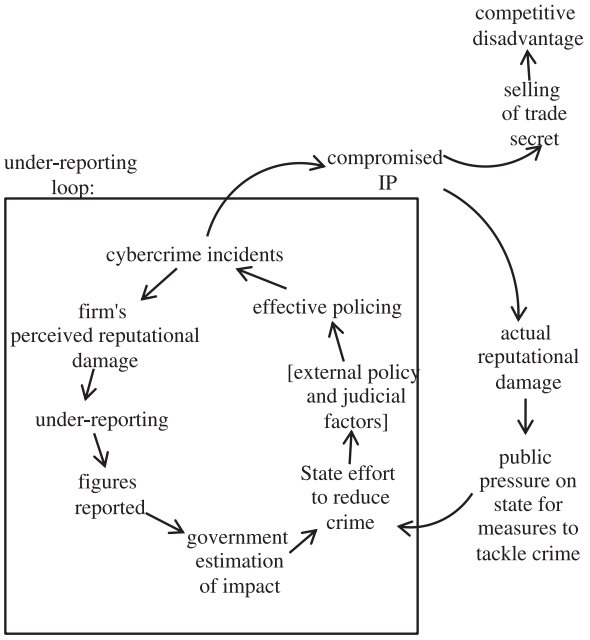

Fig. 1. Under-reporting loop adapted from Lagazio et al (2014).

lic. We then illustrate some of our results with case analyses followed by a policy discussion.

3. Conceptual framework

We model a game theoretic interaction between a victim firm and a government security agency, in our case the FBI, to explore cases arising from the theft of trade secrets following a cyber breach. This model informs our conceptual framework as we better understand the firm's investment in cyber security, their decision-making process in reporting to the FBI, and the FBI's strategy in determining investigations.

Our choice of game theory as a methodology sits among existing applications of the economics of crime theory to cybercrime. The classic Beckerian (Becker, 1968) model of crime incorporates cost-benefit analyses from the perspective of criminals, victims, and society. In this context, the economics of conventional crime can be applied to cybercrime, but operate in the relatively underdeveloped judicial context of cybercrime (Moore et al., 2009). Models are important to our chosen topic as empirical evidence is not often available for cybercrime (Lagazio et al., 2014) and trade secrets (Hall et al., 2014), largely due to data challenges. Existing theoretical models provide extensive analysis of user behavior, but there is a lack of integrated models that incorporate more types of players (Manshaei et al., 2013). The literature has generally focused on deterrence in cyber security (Hua and Bapna, 2013), which is more effective when the probability of conviction increases, rather than the punishment itself (Becker, 1968; Kshetri, 2006). Analysis of a criminal's expected utility and a victim's decision-making is relatively widespread. However, the relationship between victims and society, as mediated by government policy, is underdeveloped; we address this gap in the literature.

Two key questions to better understand cybercrime and economic espionage are: (1) what are the optimal levels of private and public investment in detection and prevention of theft (cyber security)?, and (2) what is the optimal level of investment in deterrence via the expected punishment (detection and punishment levels)? Becker (1968) frames the social loss from crime as a function of damages, costs of apprehension and conviction, the social cost of punishment, and the number of offenses. Our focus allows us to analyze FBI strategy to reduce the social loss of cybercrime by encouraging private investment in protection (cyber security). The expectation is private investment is efficient both in terms of reducing the supply of offenses and damages, and a more efficient balance of public versus private expenditures.

3.1. Applying Becker

To structure our analyses, we develop Becker's analysis of apprehension and conviction (public expenditures), and protection and apprehension (private expenditures). We take as given the remaining three elements of Becker's model: damages, supplies of offenses, and punishments, in order to focus on public policy aspects related to cybersecurity. This focus necessarily reduces the role of the criminal in our framework, by assuming a fixed supply of crime. Becker models this supply on the would-be criminal's expected utility (EU) of the crime, which weighs expected income against the expected punishment of the crime. The severity of punishment is less important than the probability of conviction. We implicitly include Becker's supply of crime by addressing the latter, as influenced by the interaction between the firm and the FBI.

Our conceptual framework examines private and public expenditures. Becker notes that the cost (C) to 'apprehend and convict' criminals is a function of activity (A) and increasing in A. A, the total activity of apprehending and convicting offenders, is inversely related to the level of crime; as A rises, the level of crime decreases. A itself is a function of manpower (m), resources (r) and capital (c). These relationships are summarized in Eq. (1).

The cost of apprehension and conviction

$$C = f(A)$$
$$\text{Where } A = f(m, r, c)$$
$$C' = \frac{dC}{dA} > 0 \tag{1}$$

However, the benefits or reduced losses of less crime are offset against the costs (C) of this activity. As per Eq. (2), C can also be expressed as the sum of public expenditures (C_{public}) and private expenditures ($C_{private}$), where $C_{private}$ in our case is the sum of expenditures of all n firms in the economy (C_{firm}). The relationship of these expenditures, in the context of Becker's model, describes the delicate ecosystem in which the overall objective is an efficient level of social loss that balances costs and benefits.

Breakdown of costs

$$C = C_{public} + C_{private}$$
$$C_{private} = \sum_{i=1}^{n} C_{firm_i} \tag{2}$$

The challenge for the FBI is that it must gauge the correct C_{public} in order to achieve this efficient outcome. Yet without knowledge of the level of theft, the government is unable to both judge ex ante C_{public} and ex post pursue theft, leading to an inefficient level of punishment and deterrence. However, as Becker (1968) notes, echoed by Png et al. (2006), private expenditures (such as 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). For example, a firm may seek to shift their own costs to C_{public} by relying on the judicial system even when private options may be more appropriate (Wagner, 2011). Equally, in our cybercrime environment, the firm may freeride on the herd immunity created by other firms, $C_{private}$. This misalignment between the incentives of the individual firm, C, and social loss again supports the FBI's policy to encourage private investment in cyber security, $C_{private}$. These competing preferences and relationships are visualized in Fig. 2.

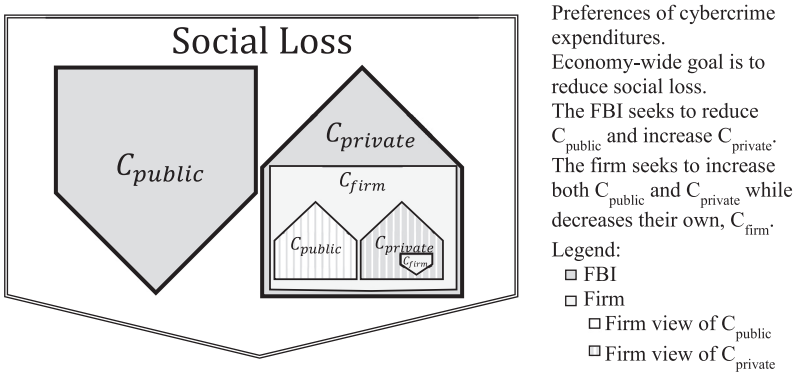

Fig. 2. Visualization of competing preferences in determining C.

This framework is riddled with asymmetries of information. Our interest is the asymmetries between the decision makers setting the level of public and private expenditures (C), in reference to the activity of the FBI and the cybercrime victim firm. Becker also notes that total activity A can be approximated by the number of convictions, as displayed in Eq. (3). This estimation multiplies p the ratio of offenses cleared by convictions to all convictions, and the activity level of offenses O. The challenge for the FBI, however, is that without reporting by firms, information asymmetries mean they have limited information on O, and therefore are ill equipped to estimate p.

Approximating activity

$$A \cong pO \tag{3}$$

To investigate these relationships, we concentrate on the fallout of a cybercrime in the theft of trade secrets. We examine the focused interactions of two players (the FBI and a victim firm) following a case of cybercrime. In this case, the firm must decide whether or not to report the crime, and the FBI must decide how to allocate their resources. This targeted examination gives us insight into the wider challenges of setting the efficient levels of activity. It necessarily looks at the focused interactions of two players, in one instance, as part of the wider game, so that we can develop a conceptual framework.

3.2. Game theoretic model

Using Becker to motivate our game-theoretic signaling framework, we develop the game is represented in Fig. 3. The sender is a firm. This firm can be of two types with respect to their cyber security investment (C_{firm}): Type H (t_H) has a high security cyber environment and Type L (t_L) has a low security cyber environment. Nature chooses the type, where the likelihood of a high security firm is P(H) = α. Either type of firm can report (R) an exogenous breach (i.e. the theft of a trade secret) of their cyber security environment. They may also choose to not report (NR) a breach. The firm's message space is therefore m = (R, NR). This report signal is received by some government security agency (the FBI). This agency does not know whether the report is from a H or L type firm. However, the agency must decide to place a high or low priority 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, which drives the agency's likelihood of placing a high priority on following up on a report. If the government agency believes a report comes from a high security type firm, then it will place a high priority (HP) on the report. On the other hand, if it believes that the report emanates from a low security firm it will place a low priority (LP) on investigating the report. The agency cannot take any action (NA) in the absence of a report. The government security agency's action space is therefore a = (HP, LP, NA).[9]

The players have preference ordering over their actions. The firm's utility function $U_{iF} = U^{a}_{jF,m}(B_{jF},\ C_{public},\ C_{firm_i},\ r\sum_{i=1}^{n} C_{firm_i})$ where j = (H, L) and P(H) = α; $a = (HP,\ LP,\ NA)$, and B_{jF} is the benefit to the individual firm from investing in security. Note that the individual firm's utility depends not only on its' own investment in cybersecurity but also the overall private investment in cybersecurity. In other words, there are positive externalities from this private investment that increases B_{jF}.

The government security agency's utility function is $U_S^{a,jm} = U_S^{a,jm}(B_S,\ C_{public},\ C_{private})$ where j, m, and a are defined above. B_S is the social benefit from the government agency's actions. $C_{public}, C_{private}$ are defined above. The usual assumptions of rationality apply to these utility functions. This is required of the sequential rationality needed to use Bayesian Nash as an equilibrium refinement as well as use expected utility as a part of a Nash solution concept (see e.g. McCarty and Meirowitz, 2007, pp. 20–22 and pp. 210–212).

Above we have developed a pared back model to lay out the information structure that we seek to investigate. In what follows, we apply this model to a specific and stylized example to illustrate how this model can be applied to the asymmetric information problem we highlight. We model two circumstances for comparative analysis. In one case, the breach goes public whether the firm reports it (R) or not (NR). In the other case, the breach only goes public if the firm reports it and *not* if it does not. This allows us to use our model to analyze whether publicity about breaches influences a firm's tendency to report breaches and the security agency's desire to investigate breaches, and implications for $C_{public}, C_{private}$.

A different analysis could be performed with a different question in mind by changing the preference ordering of the players. As it is, the structure of the game lends itself to solutions using subgame perfection as well as Bayesian Nash. Further research using open source software like GAMBIT could be used to derive many different equilibria arising out of other preference orderings that reflect other lines of inquiry. Alternatively, such an approach could

[9] In this paper, our focus is on creating a framework for understanding information asymmetries between the government security agency and the firm as it relates to public and private investment in cybersecurity. We therefore keep the choice of security level exogenous and binary. We recognize that this decision itself is endogenous to the likelihood of a cyber-attack which in turn depends on firm and security agency investment, among other things. However, this circular chain of causality is difficult to model. Moreover, the strategic interaction between the cybercriminal, the firm, and the security agency can be cast as a different problem. Basuchoudhary et al. (2015) focus on this latter problem by modeling firm security investment as a passive defense by firms, and government security agency action as an active defense involving detecting and punishing cyber criminals.

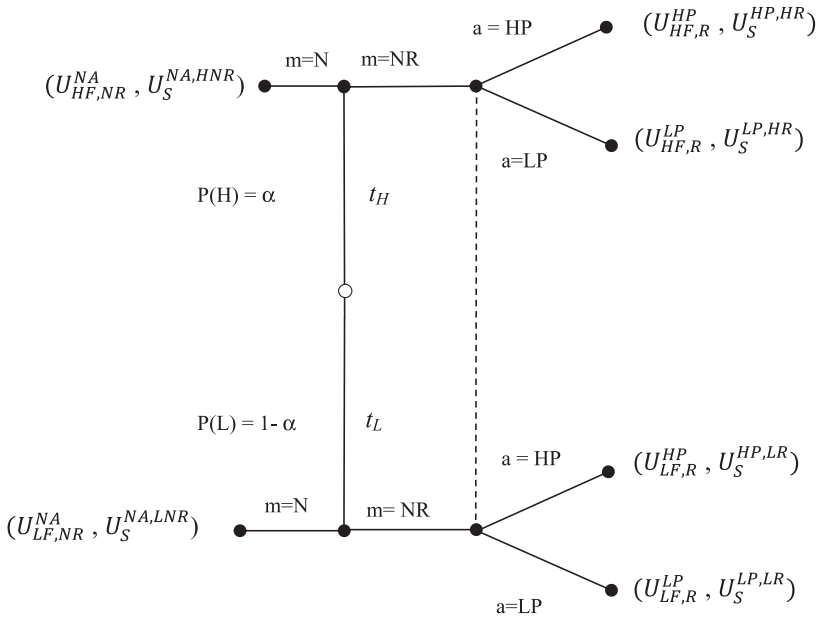

Fig. 3. The signaling game.

Table 1
Action, belief, and payoff tables for government security agency (Player 2).

Player 2	Action	Belief	Utility
Government security agency	Hi-priority conditioned on reporting	Report originates from high security firm	$U_S^{HP,HR}$
Government aecurity agency	Low-priority conditioned on reporting	Report originates from high security firm	$U_S^{LP,HR}$
Government security agency	Hi-priority conditioned on reporting	Report originates from low security firm	$U_S^{HP,LR}$
Government security agency	Low-priority conditioned on reporting	Report originates from low security firm	$U_S^{LP,LR}$
Government security agency	No Action	Low security firms do not report	$U_S^{NA,LR}$
Government security agency	No Action	Low security firms do not report	$U_S^{NA,HR}$

also determine the sensitivity of equilibria to plausible assumptions about preferences (Searle and Basuchoudhary, 2019). Thus, our model is flexible for different analyses. In this paper we focus entirely on one such example; whether public knowledge about a breach matters or not by noting equilibrium changes in two situations, first where any breach becomes public knowledge and then when only reported breaches become public knowledge.

4. Example: reporting cybercrimes and public and private resource allocation to security – does publicity matter?

Above, we combined existing strands in the cybercrime literature to highlight a theoretical gap in our understanding of cyber security breaches and trade secrets. Specifically, how does a security agency's decisions to investigate a theft of trade secrets interact with a firm's decision to report the crime and its decision to invest in security? In this section we apply the model developed in the previous section to answer this question within a stylized example where we compare two scenarios. In one scenario all breaches go public; in the other only reported breaches go public. The action, belief, and payoff structures of the two players in our model are presented in Tables 1 and 2. The preferences in these payoff structures is an example of how certain real-world features can be incorporated in our model (and not others). The rationale behind these assumptions are laid out in Appendix 1.

As noted above our example 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 by deriving Nash equilibria. Each case informs equilibrium outcomes, which we represent as Hypotheses. The Hypotheses in turn may have dynamic consequences, which are not necessarily in equilibrium, which we present as implications.

Table 2
Action and payoff tables for firms (Player 1).

Player 1	Player 1 Action	Player 2 Action	Utility
High-security investment	Report	High-Priority	$U^{HP}_{HF,R}$
High-security investment	Report	Low-Priority	$U^{LP}_{HF,R}$
High-security investment	Does not report	No action	$U^{NA}_{HF,NR}$
Low-security investment	Report	High-Priority	$U^{HP}_{LF,R}$
Low-security investment	Report	Low-Priority	$U^{LP}_{LF,R}$
Low-security investment	Does not report	No action	$U^{NA}_{LF,NR}$

Case 1. The security breach goes public.

In this case, a security breach goes public *irrespective* of whether a firm reports it or not. Here, the security agencies preference ordering is are $U_S^{HP,HR} > U_S^{LP,HR} > U_S^{NA,LNR} > U_S^{NA,HNR} > U_S^{LP,LR} > U_S^{HP,LR}$ while the firms' are $U^{HP}_{HF,\,R} > U^{LP}_{HF,\,R} > U^{HP}_{LF,\,R} > U^{LP}_{LF,\,R} > U^{NA}_{HF,\,NR} > U^{NA}_{LF,\,NR}$. The rationale behind such a preference ordering is explained in Appendix 1. We derive the pooling equilibrium that arises in this case, where all firms report a breach and the government security agency always places a high priority on a report if α is greater than a certain non-zero threshold, in Appendix 2. This equilibrium is restated in Hypothesis 1.

Hypothesis 1. If security breaches go public, security agencies will place a high priority for investigating a breach iff α is larger than a certain threshold denoted α^*.

Notice that Hypothesis 1 drives a government agency's cost allocation decisions. Beliefs about the likelihood a firm will adopt

high security at some cost C_{firm_i} drive $C_{public.}$ The government therefore should have a stake in promoting private investment in security to protect trade secrets.[10] This is in line with the 2018 National Cyber Strategy of the United States and the 2013 Administration Strategy on Mitigating the Theft of U.S. Trade Secrets.

Hypothesis 1 has dynamic effects. The fact that all breaches go public counterintuitively creates a space (if α is below the threshold defined in (3)) where the security agency is unlikely to place a high priority on any report regardless of the security level breach. One possible dynamic effect of such a situation could disincentivize firms from choosing high security in the first place and further depressing α.[11] Akin to Lagazio et al (2014), 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. To be specific, notice that the threshold value α^* rises as the payoff $U_S^{LP,HR}$ rises. In short, as the cost of missing out on winnable cases falls, *ceteris paribus*, the government agency is places high priority on cases for a smaller, and therefore realistically less likely, range of α. For example say at first the threshold value of α is 0.2. Then as $U_S^{LP,HR}$ rises say this threshold value rises to 0.7. Now a higher proportion of H firms are necessary to initiate a high priority response by the government agency. Thus, a rising $U_S^{LP,HR}$ may lead to fewer high priority responses by the government agency. In a dynamic setting, this disincentivizes a firm to invest in higher security. This leads to Implication 1.1.

Implication 1.1. If a security agency has lower costs from assigning low priority to a high security firm, firms avoid investments in high security when all breaches go public.

Indeed, to better allocate resources, a policy response may be to force firms to reveal their security investment on pain of punishment given the incentive structure where all security breaches ultimately go public. Currently, the FBI reporting process requires disclosure on protection measures; an insufficiently protected trade secret is not a trade secret. Our model likewise suggests the security agency's ability to allocate resources is critical for public safety. If more firms are not incentivized to invest in higher security (C_{firm}) the FBI may choose to place a low priority on cybercrime generally. This would embolden criminals and place a pall on economic activity. This leads to Implication 1.2.

Implication 1.2. Firms should bear a greater share of the responsibility of protecting themselves than a government agency when breaches go public.

Case 2. The security breach does not go public if unreported.

We have assumed the security agency is indifferent to whether a breach goes public or not, focused as they are on catching criminals rather than controlling the media. Thus, the security agency's preference ordering remains the same as in case 1. However, the firms payoff preference ordering in this case, as described in Appendix 1, is $U_{HF,\ R}^{HP} > U_{HF,\ NR}^{NA} > U_{HF,\ R}^{LP} > U_{LF,\ NR}^{NA} > U_{LF,\ R}^{HP} > U_{LF,\ R}^{LP}$. This preference ordering leads to a separating equilibrium derived in Appendix 3. In this equilibrium, only high security firms report a breach and the security agency always places a high priority on any report. This is restated in Hypothesis 2.

Hypothesis 2. Low security firms never report a breach while high security firms always report a breach if breaches can be kept secret. In this case, the government agency always assigns high priority to any reported breaches.

Hypothesis 2 suggests that the ability to keep breaches secret may actually lead to more efficient resource utilization for the government agency. Low security firms have an incentive to keep breaches secret. But this dynamic would encourage hackers to target low security firms. Which would create a private incentive for low security firms to adopt high security as well. This leads to Implication 2.1.

Implication 2.1. As long as unreported breaches are secret, firms have an incentive to adopt high security.

Hypothesis 1 and its implications suggest firms may underinvest in high security when breaches go public. Whether they do depends on the proportion of firms that choose high security and consequently the likelihood a security agency will place high priority on a security breach at a high security firm. Firms avoiding the high cost of public scrutiny if they chose not to report a breach drive this dynamic.

Hypothesis 2 on the other hand suggests that if firms can keep breaches private by *not* reporting, then only high security firms will report a breach. This makes it easy for the security agency to give a high priority to all reported reaches. The security agency prefers this latter scenario because it directs resources toward breaches that can be resolved positively. In turn, such directed resources would increase the likelihood that low security firms adopt high security. Hypothesis 2 and its implications therefore create a positive incentive for firms to adopt high security.

Hypothesis 1 and 2 show that a firm's incentive to invest in high security is contextual and leads us to Hypothesis 3.

Hypothesis 3. A firm is more likely to invest in high security when security breaches can be kept private.

We present two cases in the section below. We note however that while in principle all our Hypotheses are testable, in practice some of the information may not be available to the impartial observer. We focus on Hypothesis 1 to reveal this possibility in the cases below. We reiterate that the game theoretic methodology reveals mathematically logical implications for firms and security agencies from certain contexts, for example, going public or not. These implications, being mathematical, are precise and therefore more precisely falsifiable. Thus our game theoretic framework may be a helpful tool to explicitly bring science into the debate over cyber security/trade secret policy.

4.1. Case studies

Applying our framework to the real world, this section examines two court cases prosecuted under the U.S. Economic Espionage Act. Both cases are examples of industrial espionage where defendants are alleged to have bypassed cyber security controls and accessed their former employer's trade secrets. We address Hypothesis 1 and its corollaries as it assumes breaches become public and is therefore observable. As Hypothesis 1 argues, when all security breaches go public, the FBI places high priority on all reported cases if the proportion of high security firms reaches a threshold.

Our first case study, in the financial sector, demonstrates the interplay between a bank and the FBI. Sergey Aleynikov (US v. Sergey Aleynikov, 2010) was employed by the investment bank Goldman Sachs as a computer programmer for their high-frequency trading platform. In 2009, Aleynikov left to work for a competitor expanding into high-frequency trading, and was subsequently accused of stealing Goldman coding. The FBI and the federal US court system devoted extensive resources to prosecuting Aleynikov in court proceedings that eventually failed. The federal case had a number

[10] Nevertheless, we recognize that whether self-interested *individuals* in government have an incentive to promote private high security or not is an interesting exercise in political economy in its own right.

[11] We do not model this endogeneity here, but it seems like a plausible inference.

of twists, as the original prosecution was overturned on technical points.[12] A later New York state case convicted Aleynikov in 2018.

Breaches in the financial sector may be more likely, globally, to become public. The sector is highly regulated and has more obligations related to data breaches than other sectors.[13] These regulations shift more responsibility onto the firm (Implication 1.2) and mean that a firm suffering a breach can be legally required to make the breach public. Thus, we can conclude that our assumption that breaches go public (or are at least more likely to go public) can be applied.

In the case above, Goldman Sachs reported (R) the theft in July 2009. The time from Goldman Sachs reporting to the FBI and Aleynikov's arrest was two days. The speed at which Goldman Sachs pursued action suggests they expected the loss of the trade secret to have an immediate impact on the business, and the breach likely to become public. Goldman Sachs, a large bank with extensive political ties, convinced the FBI to pursue HP. As Wagner (2011) argues, "[victims with] strong existing ties to the federal government…could determine if the relevant wrongdoers will be criminally pursued."[14] Under R and HP, Goldman Sachs's payoffs were either $U^{HP}_{HF,\ R}$ or $U^{HP}_{LF,\ R}$. Both $U^{HP}_{HF,\ R}$ and $U^{HP}_{LF,\ R}$ are greater than non-reported (NR) outcomes in the event the theft goes public. However, given HP, only $U^{HP}_{HF,\ R}$ is greater than NR outcomes when the theft does not go public, as $U^{NA}_{LF,\ NR} > U^{HP}_{LF,\ R}$. From the choice to report (R), we can infer that Goldman Sachs self-assessed as H, although the discussion below questions this.

As per the second part of our Hypothesis 1, the FBI adopted HP. Court documents[15] describe the urgency with which the government pursued action, based on the assumption that the code could swiftly be used to create a functioning trading platform. The extensive government action following the FBI investigation also supports the argument that the case was treated as a priority. Returning to Hypothesis 1, the FBI may globally assume that α in the financial sector, a relatively security-conscious sector, meets the threshold α^*. Consequently, the FBI likely assessed Goldman as H and assigned HP. Court documents also describe the government as relying heavily on Goldman Sachs's self-report in a manner that, according to the defendant's lawyers, was atypical.[16] This suggests that the FBI had limited information as to whether Goldman Sachs was L or H.

Goldman Sachs may not, however, have been Lewis (2013) calls Goldman Sachs's security into question and discusses arguments that much of the stolen code was open source. Goldman Sachs's response to Lewis (2013, p.1) argues instead that, "the firm has put in place extensive safeguards to protect this valuable technology." However, the status of Goldman Sachs as either H and L in practice may be moot, the allocation of HP suggests the FBI assessed Goldman's cyber security as H.

The outcome of the Goldman Sachs case is an instance where the FBI chose HP, but it is unknown whether Goldman Sachs was H or L. The FBI's choice of HP also likely considered wider issues such as the reputation of the NY Financial Sector. Indeed, the prosecutor in the New York state case argued, "no company wants to do business in a market where someone can steal its work product without implications" (Stempel, 2017, p. 1). Nonetheless, the FBI investigation resulted in the FBI's worst payoff ($U^{HP,LR}_{S}$) – because although the FBI chose to assess the case based on HP, the case was unsuccessful in terms of securing a conviction.

Goldman Sachs fared slightly better, as it eventually reached $U^{HP}_{LF,\ R}$ (its third best payoff in a scenario where a case goes public) given the lack of conviction and assuming L. However, the success in the NY v. Aleynikov state case means Goldman Sachs effectively ended at $U^{HP}_{HF,\ R}$, its highest payoff. (The same is not true for the FBI as it only deals with federal cases.) This case also demonstrates that Goldman Sachs successfully leveraged Becker's C_{public} to augment, or even offset, the firm's investment in security (C_{firm}). In both scenarios, Goldman Sachs successfully in leveraged C_{public} to its benefit.

Our second case provides further insights into Hypothesis 1. The two defendants, Jared Sparks and Jay Williams (USA v. Sparks et al. 2016), worked for LBI Inc., a contractor for the US Office of Naval Research (ONR) (part of the Department of Defense (DOD)), from 2010 to 2011 designing unmanned vehicles. Sparks and Williams left LBI to join another ONR contractor, Charles Rivers Analytics (CRA), a larger competitor expanding into unmanned vehicles. Before leaving LBI, the defendants transmitted LBI documents to CRA. LBI lost $2.7M[17] in contracts as a direct result of the trade secret theft. In 2018, Sparks was found guilty while charges against Williams were dismissed.

Like the financial sector, the defense sector is highly regulated. Cyber security requirements for DOD contractors are rigorous.[18] DOD contractors are required to report suspicious activity; ten percent of contractors file a report in a given year.[19] It is reasonable to assume that breaches in the defense sector typically become, at least in part, public (some may be restricted due to security concerns.) Furthermore, it is reasonable to assume that the proportion of firms with high security (α) is relatively high.

At the time of the theft in 2011, however, DOD cyber security requirements were inconsistent,[20] and the FBI would not have been able to take it as given, *a priori*, that LBI was H. However, the FBI may have expected LBI to be more likely H than L ($\alpha > 0.50$). Court documents refer to LBI as having, "reasonable measures to protect and keep secret its proprietary information as well as to protect the integrity of its physical equipment and electronic files" (Indictment, p. 6) .[21] Yet the relatively unsophisticated manner of the document transmission (using the cloud storage service DropBox), suggests that while the protection may have been reasonable, it was not particularly effective.

LBI was obliged to report (R). The loss of both the $2.7 M contract and the competitive advantage of the innovations documented in the stolen prototypes and drawings negatively affected LBI, a relatively small firm. This compounds its disadvantage when competing with the larger CRA in government tenders and makes it even more resource-limited in pursuing civil redress. Pursuing criminal redress may abate these negative impacts and address reputational concerns as signaling H demonstrates LBI's trustworthiness as a contractor.

The outcome is mixed as the defendants received different outcomes from their jury trials. Williams was charged but then ac-

[12] This finding was on the grounds that the source code was not physical property and further that the code did not meet the economic espionage requirement as no foreign commerce came into play.

[13] For example, the Financial Modernization Act of 1999 which makes banks liable for data breaches and fines associated with Payment Card Industry Data Security Standard.

[14] p. 1032

[15] Doc 35 "Memorandum Of Law In Support Of Defendant's Motion For Court Approval, Nunc Pro Tunc, To Subpoena Documents And Materials From Goldman Sachs & Company" in (2010) 3:16−cr−00198−AWT−1, USDC SDNY.

[16] Doc 35 "Memorandum Of Law In Support Of Defendant's Motion For Court Approval, Nunc Pro Tunc, To Subpoena Documents And Materials From Goldman Sachs & Company" cited in (2010) 3:16−cr−00198−AWT−1, USDC SDNY.

[17] Case 3:16-cr-00198-AWT Document 388-7 Filed 08/20/18.

[18] E.g. The 2016 Federal Acquisition Regulation (FAR) sets out minimum security standards and introduces a 72-hour reporting window for cyber security incidents.

[19] Office of the National Counterintelligence Executive (ONCIX). (2011) Foreign Spies stealing U.S. Economic Secrets in Cyberspace, Accessed October 18, 2018 https://www.hsdl.org/?view&did=720057.

[20] Cyber security standards for Department of Defense contractors were inconsistent and largely addressed in individual contracts and guidelines until the adoption of new standards in 2013.

[21] Case 3:16-cr-00198-AWT Document 1 Filed 11/03/16.

quitted of seven counts; Sparks was charged with 21 counts and found guilty on 13. On balance, it appears that case was H and HP, resulting in $[U^{HP}_{HF,\ R},\ U^{HP,HR}_{S}]$ as the outcome. Coupled with the expectation that these cases go public, this again supports our Hypothesis 1. The FBI's decision to investigate the alleged theft may have also been influenced by the fact that LBI works in a political sensitive area – defense. The FBI may have afforded HP to the case both as a combination of their assessment of α and the nationally strategic nature of the case.

According to an FBI press release at the conclusion of the case, "Preventing intellectual property theft is a priority of the FBI's criminal investigative program. The key to this successful prosecution was due to linking considerable resources and collaboration of the private sector, federal law enforcement partners, the U.S. Attorney's office and the Criminal Division's Computer Crime and Intellectual Property Section" (DOJ, 2018, p1). In Beckerian terms, this case demonstrates how C_{public} can be important for smaller firms like LBI; these firms may not have the resources to pursue civil litigation of the theft of their business secrets. This also provides a nuance to implication 1.2 in that the size of the victim firm may influence how much responsibility it should bear in protecting secrets.

4.2. Policy implications

In the fight to reduce the level and impact of espionage and trade secret theft via cybercrime, the FBI encourages improved security at the firm level, with $C_{private}$ offsetting C_{public}. Our case studies support Hypothesis 1 – where breaches go public, and the FBI has assessed victim firms as meeting a H threshold (α^*), and therefore place HP on reports. A high security firm is in a good position even if they are in Case 2, where breaches do not go public, as they still report and still receive high priority from the FBI (Hypothesis 2). Paradoxically, Hypotheses 1 and 2 suggest a firm is *more* likely to invest in high security if the breaches can remain secret (Hypothesis 3.) Thus, regulations requiring the reporting of theft, data breaches and financial details to encourage disclosure, thereby creating an environment where breaches become public, may decrease private incentives to invest in security. This section discusses potential policy measures.

Government agencies seek the disclosure of cyber breaches to inform evidence based-policy making (better estimate p and O) and assist with allocation of resources. These agencies also seek to increase $C_{private}$ relative to C_{public}. These goals are at cross-purposes as Hypothesis 3 suggests firm is *more* likely to invest in high security when security breaches can be kept private. For example, as per Fig. 4: The underinvestment and disclosure loop, a policy that increases the number of reports makes it more difficult for the agency to distinguish between L and H. Thus, in this scenario the agency assigns more cases LP. This would result in more failed prosecutions, reducing the incentives to invest, and therefore taking α below the threshold α^*. Ultimately, the agency pursues less cases resulting in more breaches over time. To break this cycle, we argue that reporting firms should be forced to reveal their type (H or L). If unreported breaches remain secret, firms have an in-built incentive, without a policy intervention, to adopt H. This implies policy interventions to force disclosure could undermine a private incentive to invest.

If governments choose to prioritize the reporting of crime, a potential policy measure to increase disclosure could be a mandatory criminal reporting law. Orozco (2012) proposes such mandatory reporting of suspected trade secret theft,[22] and argues it would encourage better data security. However, the introduction of a requirement to report could discourage the use of trade secrets in the first place, in addition to avoiding the creation of negative externalities such as limiting civil liberties.

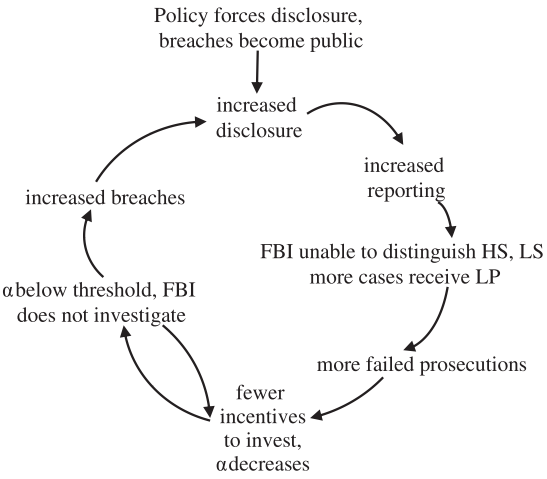

Fig. 4. The underinvestment and disclosure loop: the implications of forced disclosure.

Existing financial reporting regulations, such as the reporting requirements of listed companies, could be a policy lever to both encourage disclosure and encourage security investment. The U.S. Securities and Exchange Commission (SEC) annual 10-K form for filing firms includes a section on speculation and risk, where cyber security breaches can be reported. Hilary et al. (2016) find that the use of this section has increased modestly over the period 2010–15. While our model does not involve making C_{firm} public, security spending could become part of standard reporting requirements providing an incentive for a firm to spend appropriately. Where firms have chosen to include valuations of IP on their balance sheets, the loss of secrecy through theft requires an adjustment to the balance sheet. Insurers may also play a role in reporting requirements, as policies can require disclosure to the insurer when secrecy is affected.

Further possibilities exist under data protection laws. Existing privacy protection laws address personal data, which can fall under trade secrecy. In the event of a cyber security breach resulting in the theft of such data, firms could be obligated to disclose the theft. The finance and defense sectors are already subjected to such regulations. Existing disclosure policies in data breaches are estimated to reduce identity theft by six percent (Romanosky et al., 2011) and increase investment in cyber security (Burstein and Mulligan, 2007). Yet Hilary et al. (2016) find that US policies to encourage disclosure have led to only a modest increase in disclosures. However, disclosure regulations increase costs to business. Thus, in addition to creating an environment matching Hypothesis 3, increased regulations may perversely reduce the ability of a firm to devote resources to cyber security.

An existing policy measure for addressing investment in security is that the courts redefine "reasonable protection" with respect to cyber security in order to qualify for trade secrecy. If the bar is set higher than current levels of protection, then firms will be incentivized to invest in cyber security in order to protect their trade secrets. This could achieve the FBI's goal to encourage investment and reduce theft, without impacting 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 and not government policy. Following trends in litigation, lawyers are advising clients to adopt the US National Institute of Standards and Technology frameworks as

[22] The authors limit this to outbound trade secret theft, where the trade secret is taken from the firm. This is opposed to inbound theft, when a stolen trade secret is brought into the firm.

a standard (Shackelford, 2016). Yet standards quickly become obsolete and it may be necessary for legislation to clarify 'reasonable' (Cash, 2015). Furthermore, the court need not consider the wider 'herd-immunization' implications, which could result in the bar being set below the socially efficient level.

5. Conclusion

Our analysis brings together existing strands in the cybercrime literature to present a theoretical gap in our understanding of decision making in trade secrets protection. That is, asymmetric information problems between firms and government agencies influence public and private investments in cybersecurity. We attempt to fill this gap with a signaling game where preferences of the firm and the government agency are determined in the Becker crime and punishment framework. We then apply this model in a specific example where we analyze the incentives for investment decisions in two scenarios; one where all security breaches go public and another where only reported breaches go public. We then show how some results of this application are plausible in realistic settings and discuss policy implications. We suggest that, to the extent our model captures a fundamental asymmetric information problem between victims of a security breach and government agencies, it can be used to analyze other problems as well.

In pursuing our illustration, we find that when unreported breaches inevitably become public, the security agency might never choose to place a high priority on any report. This scenario may generate a vicious cycle where an increasing number of 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, a firm that chooses to invest less in security will never report a security breach, while a firm with high security investment will always report a breach. In the separating equilibrium that follows, 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 higher security. Thus, publicity may paradoxically enhance the likelihood of adverse selection and worsen the security environment in for trade secrets 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 introduce scenarios where 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 room for empirical exploration of our theory; differences between jurisdictional approaches to data breaches and trade secret theft may serve as natural experiments to test our policy conclusions. Our methodology reveals several testable hypotheses with implications for how policy may influence (sometimes unhelpfully) firm investments in cyber security. Further empirical understanding of firms' cyber security investment decisions may therefore provide nuance.

While we have focused on the FBI's goal of increasing private investment cyber security ($C_{private}$), 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. The FBI could choose direct action to reduce EU by increasing p through increasing C_{public} or increasing f through government legislation. These Beckerian policy options merit further exploration and could provide insights into legal and policy trends and attempts to keep jurisprudence in line with technology.

Finally, our analysis focuses on domestic policy. True 'herd immunity' requires collective efforts to encourage security; there is 'no island in cyberspace' (Shackelford, 2016). We have limited understanding of the global aspects of cybercrime and the appropriate political response. Framing the research question in an international policy context, which ironically might involve developing standards with the state-sponsors of cybercrime, could yield interesting results. 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.

Declaration of Competing Interest

The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2019.101591.

Appendix 1. Assumption driving preferences

The security agency's payoffs in order of preference are $U_S^{HP,HR} > U_S^{LP,HR} > U_S^{NA,LNR} > U_S^{NA,HNR} > U_S^{LP,LR} > U_S^{HP,LR}$. The security agency prefers to respond to H rather than L firms because the security agency wants to incentivize investment in high security by offering greater protection to such firms. The FBI and the wider judicial system have resource constraints forcing such decisions.[23] It therefore seems reasonable to seek to commit resources to firms with high security because (a) high security systems are more likely to lead to convictions because these systems are designed to better track breach processes, and/or (b) high security meets the reasonable protection threshold for trade secrecy protection, whereas low security may not and thus frustrate prosecution. Furthermore, protecting firms that did the right things is fair and appears as such to the taxpayer.

Given these parameters, the security agency prefers to place high priority on reports from a high security firms rather than a high priority on a low security firm ($U_S^{HP,HR} > U_S^{HP,LR}$). In fact, as prosecutions in the face of low security are unsuccessful[24] ($U_S^{NA,HNR}$ and $U_S^{NA,LNR}$ are preferred over $U_S^{HP,LR}$ and $U_S^{LP,LR}$) security agencies would prefer to not receive any report at all to receiving reports from a low security firm. Nevertheless, it would rather not receive a report from a low security firm than a high security firm ($U_S^{NA,LNR} > U_S^{NA,HNR}$) as it has a general preference for H as a matter of national cyber security and trade secret policy. 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

[23] Senator Coons' (Democrat-Delaware), comment (in Committe on the Judiciary, 2014) "The Department of Justice has many priorities and *limited resources*, and so it is unsurprising to me that there were just 25 trade secret cases brought last year" highlights this resource allocation problem. Likewise, "FBI cyber investigators hate to admit they're brutally overworked and must *triage* cases…" (Selby, 2017.p. 1).

[24] A higher security environment requires more extensive or sophisticated action on the part of the cybercriminal. Thus, proving mens rea (mental state of intent or recklessness in committing a crime) or similar is consequently easier in a high security environment. Furthermore, 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 et al. (2005) note that trade secrecy protection is often only determined when conflict has arisen.

($U_S^{HP,HR} > U_S^{LP,HR}$) and vice versa if it believes reports are coming from low security firms ($U_S^{LP,LR} > U_S^{HP,LR}$). The government agency finds it costly to mistakenly assign a low priority to a high security firm to incentivize firms to adopt a high security stance as a public good. Alternatively, placing a high priority on a low security firm wastes resources. The security agency's incentive structure is therefore geared to minimize security breaches by incentivizing firms to adopt a high security stance and to promote the public good; for example, promoting innovation by keeping proprietary inventions from being copied. Thus, the security agency is not concerned about the private cost to firms from economic espionage. Notice that these a priori conditions are unrelated to whether the security breach goes public or not. Consequently, whether a breach goes public or not does not affect the preference ordering of the government security agency.

Case 1: If a security breach goes public *irrespective* of whether a firm reports it or not, the firms payoff preference ordering is $U_{HF,\ R}^{HP} > U_{HF,\ R}^{LP} > U_{LF,\ R}^{HP} > U_{LF,\ R}^{LP} > U_{HF,\ NR}^{NA} > U_{LF,\ NR}^{NA}$. Breaches becoming public could reflect future disclosure regulations, particularly for listed companies and government contractors.[25] 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 would rather report than not report ($U_{HF,\ R}^{HP} > U_{HF,\ R}^{LP} > U_{HF,\ NR}^{NA}$) since our model has no advantage from hiding the breach. In fact, the low security firm would also prefer reporting in order to avoid bad publicity and the liability cost of not reporting given the assumption the breach is bound to go public ($U_{LF,\ R}^{HP}$ and $U_{LF,\ R}^{LP}$ are both $> U_{LF,\ NR}^{NA}$). We further assume $U_{HF,\ NR}^{NA} > U_{LF,\ NR}^{NA}$ because even when 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 liability faced by low security firms that failed to even try. As there is no advantage to hiding a breach – all breaches go public – reporting is generally preferred to not reporting. That is, $U_{HF,\ R}^{HP}$, $U_{HF,\ R}^{LP}$, $U_{LF,\ R}^{HP}$, $U_{LF,\ R}^{LP}$ are all preferred to $U_{HF,\ NR}^{NA}$, $U_{LF,\ NR}^{NA}$ since unreported breaches impact company value by reducing customer and shareholder trust in company management. Reporting also conveys benefits by providing a means for criminal action in cases where civil redress is ineffective (e.g., judgment-proof defendants) and, in a dynamic setting, transparency and cooperation with the FBI may convey benefits to the firm in the event of future breaches.

Case 2: On the other hand, if the security breach does not go public then the firms payoff preference ordering is $U_{HF,\ R}^{HP} > U_{HF,\ NR}^{NA} > U_{HF,\ R}^{LP} > U_{LF,\ NR}^{NA} > U_{LF,\ R}^{HP} > U_{LF,\ R}^{LP}$. 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. Thus, both $U_{LF,\ R}^{HP}$ and $U_{LF,\ R}^{LP}$ are less than $U_{LF,\ NR}^{NA}$. Nevertheless, if the low security firm did report it would prefer the security agency place a high priority on the report, i.e., $U_{LF,\ R}^{HP} > U_{LF,\ R}^{LP}$. This is a moot point, however, 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, the firm prefers a high priority by the security agency. The security agency's use of high priority will result in conviction of the perpetrators and minimize the ability of competitors to use the innovation protected by the trade secret and may even result in victim compensation paid to the firm.

However, the firm would rather not report if it believes 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. All this implies that $U_{HF,\ R}^{HP} > U_{HF,\ NR}^{NA} > U_{HF,\ R}^{LP}$. We arbitrarily assume that $U_{HF,\ R}^{LP} > U_{LF,\ NR}^{NA}$ to have a complete preference ordering. Alternatively, $U_{LF,\ NR}^{NA}$ could be $> U_{HF,\ R}^{LP}$. Either way we would have a complete preference ordering over all outcomes and have no effect on the outcome of the game. Our assumption of breaches going public if reported is a matter of reality. Assuming investigation leads to charges, court records are typically public, so action by the security agency or remedy arising from this action would be public knowledge.

Appendix 2. Establishing the Nash Equilibrium in Case 1

We start with a pooling strategy profile and then test for stability, to establish whether the chosen profile is a Nash equilibrium. In this case, the high security firm prefers $U_{HF,\ R}^{HP}$ and $U_{HF,\ R}^{HP}$ over $U_{HF,\ NR}^{NA}$. The low security firm also prefers $U_{LF,\ R}^{HP}$ and $U_{LF,\ R}^{LP}$ over $U_{LF,\ NR}^{NA}$. Both types of firms 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 high security (H) firm with α probability. Thus, it gets a report from a low security (L) 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 low priority. It then chooses the strategy with the higher expected payoff. The expected payoffs are:

$$\mathrm{E(HP)} = \alpha U_S^{HP,HR} + (1-\alpha) U_S^{HP,HR} \tag{B1}$$

and

$$\mathrm{E(LP)} = \alpha U_S^{LP,HR} + (1-\alpha) U_S^{LP,HR} \tag{B2}$$

Thus, the security agency will only place a high priority on a report if (B1) > (B2) i.e., if

$$\alpha > \left(U_S^{LP,LR} - U_S^{HP,LR}\right) \Big/ \left(U_S^{LP,LR} - U_S^{HP,LR} + U_S^{HP,HR} - U_S^{LP,HR}\right) \tag{B3}$$

Notice that (B3) is certainly plausible since it requires that α be greater than some positive fraction.[26] Thus, if α is greater than this threshold value, $\alpha^* = (U_S^{LP,LR} - U_S^{HP,LR})/(U_S^{LP,LR} - U_S^{HP,LR} + U_S^{HP,HR} - U_S^{LP,HR})$, then the security agency will always place a high priority on a report and a low priority otherwise. We have already established that both types of firms will always report a breach when all breaches go public. Neither player will deviate from this strategy profile thus establishing a stable pooling Bayesian Nash Equilibrium. Further notice that as $U_S^{LP,HR}$, rises so does α^*.

Appendix 3. Establishing the Nash Equilibrium in Case 2

In this case notice that the firm's payoff structure suggests that the L type firm will never report a security breach. In comparison, the H type firm will report a security breach if it believes the report will be accorded a high priority but not otherwise. This creates a scenario where both types of firms may not pool (always report) on reporting a breach. This opens the possibility of a mixed strategy Bayesian Nash Equilibrium. However, the solution is simpler. In this case, the fact the L firm will never report a breach means that all reports *must* be from the H firm even if some H firms choose not to report. Thus, from the security agency's perspective the likelihood that a reported breach is from a H type is 1. Given this belief, it is optimal for the security agency to always place a high priority on any reported breach. Of course, in that case the H type firm should always report. In other words, in the scenario where *not* reporting a breach never becomes public, the H

[25] To a certain extent, this is already true for military contractors as discussed in the case studies.

[26] (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.

firm will always report, the L firm will never report, and the security agency will always place a high priority on a reported breach, establishing a stable separating equilibrium.

CRediT authorship contribution statement

Atin Basuchoudhary: Conceptualization, Formal analysis, Investigation, Methodology, Visualization, Writing - original draft, Writing - review & editing. **Nicola Searle:** Conceptualization, Data curation, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Visualization, Writing - original draft, Writing - review & editing.

References

Acquisti, A, Friedman, A, Telang, R, 2006. Is there a cost to privacy breaches? An event study. In: ICIS 2006 Proc., p. 94.

Anderson, R, Moore, T, 2006. The economics of information security. Science 314 (5799), 610–613.

Anderson, R, Barton, C, Böhme, R, Clayton, R, Van Eeten, MJG, Levi, M, Moore, T, Savaga, S., 2013. Measuring the cost of cybercrime. In: The Economics of Information Security and Privacy. Springer, pp. 265–300.

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

Anson, W, Suchy, DP, Ahya, C, 2005. Intellectual property valuation: a primer for identifying and determining value. Am. Bar Assoc. J.

Anton, JJ, Yao, DA, 2004. Little patents and big secrets: managing intellectual property. RAND J. Econ. 1–22.

Arcuri, MC, Brogi, M, Gandolfi, G, 2017. How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns.

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.

Arundel, A., 2001. The relative effectiveness of patents and secrecy for appropriation. Res. Policy 30 (4), 611–624. Accessed April 4 2018 from: http://linkinghub.elsevier.com/retrieve/pii/S0048733300001001.

Basuchoudhary, A, Choucri, N., 2014. The evolution of network based cyber security norms: an analytical narrative. In: Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference on. IEEE, pp. 646–653.

Basuchoudhary, A, Eltoweissy, M, Azab, M, Razzolini, L, Mohamed, S, 2015. Cyberdefense when attackers mimic legitimate users: a Bayesian approach. In: 2015 IEEE International Conference on Information Reuse and Integration, pp. 502–509. doi:10.1109/IRI.2015.83.

Becker, G.S, 1968. Crime and punishment: an economic approach. In: The Economic Dimensions of Crime. Palgrave Macmillan, London, pp. 13–68.

Bhattacharya, S, Guriev, S., 2006. Dec. Patents vs. trade secrets: knowledge licensing and spillover. J. Eur. Econ. Assoc. 4 (6), 1112–1147. Available from: http://www.mitpressjournals.org/doi/abs/10.1162/JEEA.2006.4.6.1112.

Bulut, H, Moschini, G, 2006. Patents, trade secrets and the correlation among R&D projects. Econ Lett. 91 (1), 131–137. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0165176505003812.

Burstein, A, Mulligan, D, 2007. Security Breach Notification Laws: Views From Chief Security Officers. A study Conduct Samuelson Law Technol Public Policy Clin Univ California-Berkeley Sch Law.

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

Cash, MH, 2015. Keep it secret, keep it safe: protecting trade secrets by revisiting the reasonable efforts requirement in Federal Law. J. Intell. Prop. L 23, 263.

Cavusoglu, H, Mishra, B, Raghunathan, S, 2004. The effect of internet security breach announcements on market value : capital market reactions for breached firms and internet security developers. Int. J. Electron. Commer. 9 (1), 69–104.

Cohen W, Nelson R, Walsh J. Protecting Their Intellectual Assets: Appropriability Conditions and Why Firm Patent and Why They Do Not in the American Manufacturing Sector. NBER Work Pap. 2000: 7552.

Committe on the Judiciary, 2014. Are Our Laws Adequate for Today's Threats (Online)Serial No. J–113–59. Available from: HYPERLINK https://www.gpo.gov/fdsys/pkg/CHRG-113shrg96009/pdf/CHRG-113shrg96009.pdf.

Crass D, Garcia-Valero F, Pitton F, Rammer C. Protecting Innovation Through Patents and Trade Secrets: Determinants and Performance Impacts for Firms with a Single Innovation. 2016.

Cugno, F, Ottoz, E., 2006 Sep. Trade secret vs. broad patent: the role of licensing. Rev. Law Econ. 2 (2). Available from: http://www.bepress.com/rle/vol2/iss2/art3.

Davis, G, Garcia, A, Zhang, W, 2009. Empirical analysis of the effects of cyber security incidents. Risk Anal. 29 (9), 1304–1316. Available from: https://doi.org/10.1111/j.1539-6924.2009.01245.x.

DOJ. Electrical Engineer Found Guilty for Intending to Convert Trade Secrets from Defense Contractor. Press Release (Online). 2018 Jul 10; Available from: HYPERLINK https://www.justice.gov/usao-ct/pr/electrical-engineer-found-guilty-intending-convert-trade-secrets-defense-contractor.

Dreyfuss, R, Lobel, 2016. Economic espionage as reality or rhetoric: Equating trade secrecy with national security. O Lewis & Clark L. Rev. 20 (2), 419–476.

Ettredge, M, Guo, F, Li, Y, 2018. Trade secrets and cyber security breaches. J. Acc. Public Policy 37.6 (2018), 564–585.

Gordon, LA, Loeb, MP., 2002. The economics of information security investment. ACM Trans. Inf. Syst. Secur. 5 (4), 438–457.

Gordon, LA, Loeb, MP, Lucyshyn, W, Zhou, L, 2015a. Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. J. Inf. Secur. 6 (1), 24.

Gordon, LA, Loeb, MP, Lucyshyn, W, Zhou, L, 2015b. Increasing cyber security investments in private sector firms. J. Cyber. Secur. 1 (1), 3–17.

Gordon, LA, Loeb, MP, Zhou, L, 2011. The impact of information security breaches: has there been a downward shift in costs? J. Comput. Secur. 19 (1), 33–56.

Goverment of the United States, 2013. Administration Strategy on Mitigating the Theft of U.S. Trade Secrets Accessed January, 15, 2017 from https://www.justice.gov/criminal-ccips/file/938321/download.

Government of the United States, 2018. National Cyber Strategy of the United States of America (Online). Washington, DC Available from: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Hall, B, Helmers, C, Rogers, M, Sena, V, 2014. The choice between formal and informal intellectual property: a review. J. Econ. Lit. 52 (2), 375–423.

Hilary, G, Segal, B, Zhang, 2016. Cyber-Risk Disclosure: Who Cares? Georg McDonough Sch Bus Res Pap No 2852519.

Hua, J., Bapna S. The economic impact of cyber terrorism. The Journal of. Strategic Strat. Information Inf. Systems Syst. 22.2 (2013): 175–186.

Kshetri, N., 2006. The simple economics of cybercrimes. IEEE Secur. Priv. 4 (1), 33–39.

Kultti, K, Takalo, T, Toikka, J, 2007. Secrecy versus patenting. Rand. J. Econ. 38 (1), 22–42.

Kwon, I., 2012. Patent races with secrecy. J. Ind. Econ. 60 (3), 499–516.

Lagazio, M, Sherif, N, Cushman, M, 2014. A multi-level approach to understanding the impact of cyber crime on the financial sector. Comput. Secur. 45, 58–74.

Lewis, M., 2013 Sept. Did Goldman Sachs Overstep in Criminal Charging Its Ex-Programmer? Vanity FairAvailable from: HYPERLINK https://www.vanityfair.com/news/2013/09/michael-lewis-goldman-sachs-programmer.

Manshaei, MH, Zhu, Q, Alpcan, T, Bacşar, T, Hubaux, J-P, 2013. Game theory meets network security and privacy. ACM Comput. Surv. 45 (3), 25.

McCarty, N, Meirowitz, A, 2007. Political Game Theory: An Introduction. Cambridge University Press, New York.

McMillan, R, Olyaei, S., 2016. Identifying the real information security budget. Gart. Res.. Available from: https://www.gartner.com/doc/3400017?cm_sp=swg-_-research-_-tail.

Moore, T, Clayton, R, Anderson, R, 2009. The economics of online crime. J. Econ. Perspect. 23 (3), 3–20.

Moore, T, Dynes, S, Chang, FR, 2015. Identifying How Firms Manage Cyber Security Investment, p. 32 Available South Methodist Uni. Available from: http://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf.

Mosel, M, 2011. Big Patents, Small Secrets: How Firms Protect Inventions When R&D Outcome is Heterogeneous BGPE Discussion Paper.

Orozco, D., 2012. Amending the economic espionage act to require the disclosure of national security-related technology thefts. Cath. UL Rev. 62, 877.

Ottoz E, Cugno F. Patent-secret mix in complex product firms. 2007; American Am. Law and Economics Econ. Review Rev. 10.1: 142–158.

Panagopoulos, A, 2015. Park I-U. Patenting vs. Secrecy For Startups and the Trade of Patents As Negotiating Assets. University of Crete mimeo.

Png, I, Tang, CQ, Wang, Q-H, 2006. Information Security: User Precautions and Hacker Targeting. Natl Univ Singapore.

Png, IPL, 2017a. Law and innovation: evidence from state trade secrets laws. Rev. Econ. Stat. 99 (1), 167–179.

Png, IPL, 2017b. Secrecy and patents: theory and evidence from the Uniform Trade Secrets Act. Strateg. Sci. 2 (3), 176–193.

Png, IPL, Samila, S, 2013. Trade Secrets Law and Engineer/Scientist Mobility: Evidence from "Inevitable Disclosure." WP Nat U Singapore.

Romanosky, S, Telang, R, Acquisti, A, 2011. Do data breach disclosure laws reduce identity theft? J. Policy Anal. Manag. 30 (2), 256–286.

Rowe, EA, 2016. RATs, TRAPs, and Trade Secrets. BCL Rev. 57, 381–426.

Ruan, K, 2017. Introducing cybernomics: a unifying economic framework for measuring cyber risk. Comput. Secur. 65, 77–89.

Searle, N, Basuchoudhary, A., 2019. Does One Size Policy Fit All? The Sensitivity of Cybercrime Policy to Preferences Working paper.

Selby, N, 2017. Local Police Don't Go After Most cybercriminals. We Need Better Training. Washington Post.

Shackelford, SJ., 2016. Protecting intellectual property and privacy in the digital age: the use of national cyber security strategies to mitigate cyber risk. Chap L Rev 19, 445.

Stempel, J., 2017 Jan 24. Ex-goldman programmer's code theft conviction revived by New York court. Reuters Bus. News. Available from: https://www.reuters.com/article/us-goldman-sachs-aleynikov/ex-goldman-programmers-code-theft-conviction-revived-by-new-york-court-idUSKBN1582L0.

Von Solms, R, Van Niekerk, J, 2013. From information security to cyber security. Comput. Secur. 38, 97–102.

Wagner, RE., 2011. Bailouts and the potential for distortion of federal criminal law: industrial espionage and beyond. Tul. L. Rev. 86, 1017.

Wei, H, Frincke, D, Alves-Foss, J, Soule, T, Pforsich, H, 2005. A layered decision model for cost-effective network defense. In: Information Reuse and Integration, Conf, 2005 IRI-2005 IEEE International Conference on. IEEE, pp. 506–511.

US v. Sergey Aleynikov: 1:10-cr-00096-DLC. USDC SDNY. 2010.

USA v. Sparks et al 3:16−cr−00198−AWT−1. 2016.

Dr. Atin Basuchoudhary Professor, Virginia Military Institute Professor Atin Basuchoudhary teaches economics at the Virginia Military Institute. His work applying game theory and machine learning techniques to asymmetric information problems has been published in Decision Analysis, Public Choice, IEEE Proceedings, Defense and Peace Economics, Evolutionary Behavioral Sciences, Economics of Peace and Security Journal, and Peace Economics, Peace Science and Public Policy, among others. He has collaborated on two published books applying machine learning to predict civil conflict and growth. Prof. Basuchoudhary's research interests range from cybersecurity, to conflict economics, to the evolution of cultures. He has received grants to further research from the NSF, John Templeton Foundation, and the Charles Koch Foundation. He was interviewed about his work on National Public Radio and has been invited to speak at international venues. The Virginia Military Institute and the Commonwealth of Virginia has recognized Professor Basuchoudhary as an accomplished teacher.

Dr. Nicola Searle EPSRC Digital Economy Fellow, Goldsmiths, University of London Dr. Nicola Searle is a Digital Economy Fellow and Senior Lecturer at Goldsmiths, University of London. An economist who specializes in the economics of intellectual property, Nicola currently holds a five-year fellowship, entitled "Economic Espionage and Cybercrime: Evidence and Strategy." Her work looks at the increasing importance of trade secrets in the digital world, and the emerging threats of the theft of trade secrets and economic espionage through cybercrime. Dr. Searle is a member of the Research Council UK Digital Economy Program Advisory Board, a member of the UK Intellectual Property Office's (IPO) Research Experts Advisory Group and an Honorary Research Fellow at the School of Management, University of St Andrews. She previously held positions at the School of Design and Informatics at Abertay University. In addition to academic career, she has several years of experience as an economist in the UK government and an associate at Goldman Sachs.