ABSTRACT

Industrial cyber espionage is a growing concern amongst businesses since the trade secrets of an organization can be accessed, stored, and transmitted digitally. This research combines economic theory, deterrence theory, and cyber security to explore the economic impact of industrial cyber espionage. The research framework of using game theory helps academics and practitioners understand the important parameters in industrial cyber espionage and its economic impact.

KEYWORDS: Industrial Cyber Espionage, Espionage, Deterrence, Economic Impact, Trade Secret, Game Theory

INTRODUCTION

Espionage is the act of acquiring trade secrets, intelligence and military secrets without the permission of the owner of the information and is hence illegal. Espionage is different from intelligence gathering. In intelligence gathering, information is collected through legal and ethical means. Every year, American companies lose billions of dollars due to industrial espionage activities from foreign and domestic competitors (FBI, 2014). Addressing the theft and transfer of trade secrets overseas for innovative technology is a priority focus of the Office of the U.S. Intellectual Property Enforcement (WhiteHouse, 2013).

The concept of espionage can be traced back to more than 2000 years. Sun Tzu in the The Art of War, provided a detailed description to develop espionage capabilities for military purposes. The Byzantine emperor Justinian I (483-565) in the sixth century placed monks in China, to steal silk worms in an attempt to understand how to make silk (Fraumann, 1997). The British tea industry used espionage activities to gather the tea industry information of China, as far back as 1615 (Breed, 2003).

Some foreign and domestic companies criminally target the trade secrets of their competitors in order to gain from that information. A trade secret is any information that has value to the company because it is not publicly known. Trade secrets include formula, recipe, process, technique, method, program, device, pattern and so on, and as such are different from patents,
copyrights, and trademarks. Trade secrets of competitors can be stolen by recruiting insiders from their competitors, cyber intrusion, theft, and other methods. Today’s competitive business environment demands a comprehensive system to protect trade secrets. This paper primarily focuses on a specific espionage activity: industrial cyber espionage.

Industrial cyber espionage is the practice of obtaining trade secrets from groups, companies and governments through means of cyber attacking, which includes, but is not limited to, installing malware, hacking, social engineering, and intrusion from insiders. Industrial cyber espionage is a growing threat to the American economy (O’Hara, 2010). Because trade secrets may be in digital format and because it is difficult for victims to detect who conducts the spying operations in cyber space, foreign collectors of sensitive trade secrets can use cyber tools. Malicious software, recruiting hackers and routing through third-party countries are becoming the most popular methods used by those foreign collectors (NCIX.gov, 2011).

Kaspersky Lab, a leading anti-virus company uncovered a very sophisticated malware, Careto which predominantly targets government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organizations and activists, for espionage purposes. This malware had advanced persistent threat capabilities and bore the signature of a very high degree of professionalism in the operational procedures of the group behind this attack, and is likely state-sponsored (Hilburn, 2014). These types of malware are preferred by cyber espionage practitioners, because they can continue to compromise and steal information from victims for months or sometimes years. Careto has been in existence since 2007 and was detected only in 2014.

The focus of this paper is on industrial/economic espionage in which the victim is an organization (for-profit, non-profit) owning valuable trade secrets. The quality of anti-cyber espionage is highly related to the investments on it (Bojanc and Jerman-Blazic, 2008). The appropriate level of the espionage protection investment can enhance the capability of organizations and governments to reduce the espionage threat (Bodin and Gordon, 2005). The aim of this paper is to use game theory to analyze espionage risks and predict the behavior of competitors. This paper proposes a static game model which can be applied to different competitors. By using Nash equilibrium and other game theory concepts, this paper attempts to find an appropriate approach to study the influence of industrial cyber espionage. The rest of the paper is organized as follows. In the literature section we review the literature on the espionage research and cases, providing us with the background to propose a game theoretical model for anti-espionage investments. The game theoretical model is described in the methodology section. In the section after that, the results of simulations are analyzed. We discuss the implications of our work in the conclusion section.

LITERATURE REVIEW

In this section, we present the literature on areas that enable formulation of a model that can explain industrial cyber espionage. These areas are industrial espionage, investment in computing security, and cyber deterrence.

Industrial Espionage Cases

The following cases clearly present the threats of industrial cyber espionage in the United States. We believe that the real number of industrial cyber espionage activities is much larger than what has been reported from law enforcement agencies. Since much of the trade secrets is
stored digitally, it is also possible to copy and transfer those secrets relatively easily, compared to when the information was stored manually, as illustrated by these cases.

Case #1

In 2004, the president of Exel Transportation Services, Mr. Michael Musacchio, left Exel to form a competing company, Total Transportation Services. Joseph Roy Brown and John Michael Kelly, two other former Exel employees in Exel IT Department, also left Exel to work at Musacchio’s new company. Between 2004 and 2006, Musacchio and Brown assisted by Kelly, hacked into Exel’s computer system to conduct espionage. Through the espionage, Musacchio and Brown obtained Exel’s confidential and proprietary business information and benefited from that information. Musacchio has been sentenced to serve a total of 63 months in federal prison. (FBI, 2013).

Case #2

Yi Liu, 40, of Lexington, South Carolina, has been charged with stealing trade secrets from Sprung-brett RDI, a technology firm located in the University of Buffalo’s Technology Incubator. Liu, a Ph.D. in mechanical engineering left Sprung-brett in February 2011. For seven months following his departure, Liu retained the laptop computer that Sprung-brett had provided him while he was employed by the company. During these seven months, Liu downloaded electronic files onto an external hard drive that comprised Sprung-brett trade secrets. The charges carry a maximum penalty of 60 years in prison, a $3,500,000 fine, or both. (FBI, 2013).

Case #3

Xiang Dong Yu, a former product engineer for the Ford Motor Company from 1997 to 2007, had access to Ford trade secrets, including Ford design documents. He copied 4,000 Ford documents onto an external hard drive and returned back to China with that hard drive. Those documents include sensitive Ford design documents such as system design specifications for the Engine/Transmission Mounting Subsystem, Electrical Distribution System, Electric Power Supply, Electrical Subsystem and Generic Body Module. Ford spent millions of dollars and decades on research, development, and testing to develop and continuously improve the design specifications set forth in these documents. Yu began working for Beijing Automotive Company, a direct competitor of Ford. Yu was arrested in the U.S. and a search of his company laptop revealed 41 Ford trade secrets. Ford valued the loss of the trade secrets at $50 million dollars. In April 2011, Yu Xiang Dong was sentenced to 70 months in federal prison for theft of trade secrets and economic espionage (FBI, 2011).

Case #4

Sergey Aleynikov, a former computer programmer at Goldman Sachs between May 2007 and June 2009, was responsible for developing computer programs supporting the firm’s high-frequency trading on various commodities and equities markets. This trading system generated millions of dollars in profits annually for the firm. In April 2009, Aleynikov resigned from Goldman Sachs and accepted a job at Teza Technologies (“Teza”). He was hired to develop Teza’s own version of a computer platform that would allow Teza to engage in high-frequency trading. On June 5, 2009—his last day working at Goldman Sachs—Aleynikov transferred substantial portions of the firm’s proprietary computer code for its trading platform to an outside computer server in Germany. After transferring the files, he deleted the program he used to encrypt them and deleted his computer’s log. In addition, throughout his employment at Goldman Sachs,
Aleynikov transferred thousands of computer code files related to the firm’s proprietary trading program from the firm’s computers to his home computers, without the knowledge or authorization of Goldman Sachs. Aleynikov was sentenced in Manhattan federal court to 97 months in prison for stealing valuable, proprietary computer code of Goldman Sachs (FBI, 2011).

**Investments and Breaching Information**

Gordon & Loeb (2002) built a model that considered how the vulnerability of information and the potential loss from such vulnerability affected the optimal investment to secure that information. They proposed two classes of security breach probability functions. The first class of security breach probability function proposed was \( S^I(z, v) = \frac{v}{(az + 1)^b} \), where \( z \) is the investment, and \( v \) is the vulnerability. Their second class is not considered in this paper. The parameters, \( a \) and \( b \), are measures of the productivity of information security. The probability of breaches decreases with increases in both of these parameters. Hausken (2006) proposed a logistic breach function \( S^{III}(z, v) = \frac{v}{1 + \rho (e^{\tau z} - 1)} \) to address some of the drawbacks of the Gordon and Loeb’s breach function. Hausken’s other classes of breach functions are not considered in this paper. The parameters, \( \rho \) and \( \tau \), measure the productivity of information security. By varying the parameters of the functions, it is possible to model the sensitivity of breaching information systems to investment levels. A sensitive breach function is a function where a moderate increase in the amount of investment can decrease breaching probability considerably. In other words, a sensitive breach function has a steeper slope at a particular investment level, compared to an insensitive breach function.

**Cyber Deterrence**

Deterrence theory has been widely employed in the fields of economics and criminology to study the behavior of criminals and antisocialists (Becker, 1968; Pearson & Weiner, 1985). In criminology, deterrence theory asserts that the probability of criminal behavior varies with the expected punishment, which consists of the perceived probability of being caught and the punishment level (Pearson & Weiner, 1985). Punishment was more effective in deterring people who tried to avoid punishment or negative consequences, while ethics education was more effective in deterring people who had a strong social consciousness (Workman & Gathegi, 2007). Determining the proper punishment is an important issue in the legal field. Legal systems in most societies specify punishments that increase with the level of social harm caused by the criminal activities (Rasmusen, 1995).

Oksanen & Valimaki (2007) conducted research on copyright violations and found that the strategy of minimizing risk was not only theoretically practiced, but was also extensively used. They found that the classic deterrence model should incorporate both the reputational cost of violations and the reputational benefit of violations (Sunstein, 2003). The reputational cost means that the public lose the confidence on the offense company.

Straub & Welke (1998) considered deterrence theory as a theoretical basis for security countermeasures to reduce cyber security risks and posited that managers and administrative policies were the key to successfully deterring, preventing, detecting, and pursuing remedies to cyber attacks.

**Industrial Espionage**

Hua et al.
Industrial cyber espionage activities are targeted towards very specific companies, or industries. Since the past several years there has been an increase in the number of such targeted attacks and that such targeted attacks are most likely part of a campaign (Thonnard, Bilge, O’Gorman, Kiernan, & Lee, 2012). According to the authors, such campaigns are very sophisticated and difficult to detect.

Balduzzi, Ciangaglini, and McArdle (2013) confirm that while such targeted attacks are difficult to detect, clustering technique approach can lead to the identification of possible targeted attacks. The steady rise of Industrial espionage from 2004 to 2013 in South Korea has been documented by Lee (2013) and as a response, the South Korea police has trained police officers in the technique of digital forensics recognizing the importance of computing technology for industrial espionage. Crane (2005) documents three industrial espionage cases, one of which resulted in a lawsuit of $1 billion involving subsidiaries of two competitors, Vivendi Universal and News Corporation. In this instance, one competitor employed a “sophisticated and well-funded team of scientists” to crack the code on TV smartcards. The author states that digital information can be hacked and that such hacking can lead to disastrous consequences to the targeted company.

**METHODOLOGY**

In this research, we identify two players in our industrial cyber espionage game: the competitor and the target. Without loss of generality, the competitor may be an individual who seeks to use the trade secrets of a company. We propose a $2 \times 2$ general-sum game between a competitor and a target. The normal form of the cyber espionage game is presented in Table 1, with the rewards to the two players. A target will be a company which has valuable trade secrets and can become a victim of cyber espionage. In each of the four cells, rewards to player 1 (the competitor) are shown first, followed by the rewards to player 2 (the target company), which are negative.

Table 1 A general-sum cyber espionage game

<table>
<thead>
<tr>
<th>Player 1: Competitor</th>
<th>Player 2: Target</th>
<th>Invest More With Probability $\beta(z)$</th>
<th>No Change With Probability $1- \beta(z)$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Conduct Espionage</strong> With Probability $\alpha(z)$</td>
<td>{$\mu P_1 M - Q_1, -(P_1 M + z_1)$}</td>
<td>{$\mu P_0 M - Q_0, -(P_0 M + z_0)$}</td>
<td></td>
</tr>
<tr>
<td><strong>Do Not Conduct Espionage</strong> With Probability $1- \alpha(z)$</td>
<td>{0, $-z_1$}</td>
<td>{0, $-z_0$}</td>
<td></td>
</tr>
</tbody>
</table>
In this paper, we only define two actions which a competitor may choose. The action, “Conduct Espionage”, means that the competitor can use all possible methods to steal trade secrets from the target company. The possible cyber espionage methods may include, but is not limited to hacking, Dumpster Diving, Network Scanning, Installing Trajan Horse, Password Cracking, and social engineering. The action “Do Not Conduct Espionage” is an action where a competitor does not participate, or ceases to participate in an industrial-espionage activity.

In this paper, we also only define two actions which a target company may choose. The action, “Invest More”, means that the target invests more to protect its trade secrets. The possible protection methods may include, but is not limited to, hiring experienced cyber security professionals, monitoring insider activities, and employee education. The action, “No Change”, means that the target company won’t invest more to protect its trade secrets.

In Table 1, $P$ denotes the breach function, the probability of trade secret protection system breaches, and is a function of $z$, the target’s investment in IS trade-secret security. The variable, $M$, denotes the maximum instant loss in the incident of a trade secret protection system breach. The maximum instant loss includes any loss from incursions excluding the cost of security. Subscript 0 denotes the current state. Subscript 1 denotes the future state. $z_1 > z_0$ and $P_1 < P_0$. The variable $\alpha(z)$ represents the probability that the competitor chooses the action “Conduct Espionage”, and the variable $\beta(z)$ represents the probability that the target chooses the action “Invest More”. $H$ denotes the total reward to the competitor and $L$ denotes the total reward to the target.

- $-z_1$ is the reward to the target for the strategy pair {Do Not Conduct Espionage, Invest More}. The investment that a target makes for trade security protection is a sunk cost.
- $-z_0$ is the reward to the target for the strategy pair {Do Not Conduct Espionage, No Change}.
- $-(P_1 M + z_1)$ is the reward to the target for the strategy pair {Conduct Espionage, Invest More}. There are two costs to the target: a sunk investment cost, and a cost of losing the trade secrets. If the competitor is able to breach a system with a probability $P_1$, then the target loses $M$. Thus, the expected loss to the target is $P_1 M$. $-(P_0 M + z_0)$ is the reward to the target for the strategy pair {Conduct, No Change}.

The reward to the competitor is more complex. In Table 1, $\mu$ represents the ratio of the competitor’s gain to the target’s maximum instant loss. In other words, not all of the losses to the target will be transferred to the competitor. A competitor may not be able to utilize the stolen trade secret with the same benefit that the target could. In the perfect case of complete breaching, the gain to the competitor will be only $\mu M$. For example, if the maximum instant loss $M$ is 100 million dollars and if $\mu$ is 0.69, the reward to the competitor will be 69 million dollars, when the trade secret has been revealed to the competitor. The value range of $\mu$ is [0, 1].

Before the competitor takes action, it will evaluate its potential costs, punishment and reputational losses. We call this process as deterrence. In Table 1, the function $Q(z)$ denotes the deterrence function including the potential punishment and costs. Given that the competitor’s skills are fixed, it is assumed that

$$\frac{\partial Q}{\partial z} \geq 0$$

(1)
i.e., if the target increased investment in trade secret protection, the deterrence to the competitor would increase.

There is only one assumption concerning $\alpha(z)$, $\alpha(z = 0) = 1$. That is, if the target doesn’t protect its trade secrets at all, the probability that the competitor chooses the action “Conduct Espionage” is 100%. In Table 1, $\mu P_1 M - Q_1$ denotes the reward to the competitor, if the competitor chooses the action “Conduct Espionage” and the target chooses the action “Invest More”. $P_1(z_1)$ denotes the new probability of trade secret protection system breaches with the new investment $z_1$. $Q_1(z_1)$ denotes new deterrence which includes concerns about the potential punishment and costs of the new investment $z_1$. The deterrence function can be a linear function with variable $z$, or a constant value. The other values are treated in a similar manner with the subscript 0 referring to the target choosing the action “No Change” i.e., the target does not invest more in protecting the trade secrets.

When $\mu P M - Q = 0$, the breakeven point is represented by $z = z^*$. Boundary conditions are given next.

When $z_0 < z_1 < z^*, \mu P_1 M - Q_1 > 0$, the game reduces to a pure-strategy game. The profile of best response in the static game is: the competitor will choose the action “Conduct Espionage” regardless of the action of the target. The value of $\alpha$ is 100% until $z$ increases to the breakpoint $z^*$.

When $z_0 < z^* < z_1, \mu P_1 M - Q_1 < 0$, the game becomes a mixed strategy game. When the target chooses the action “Invest More”, the competitor will choose the action “Do Not Conduct”. When the target chooses the action “No Change”, the competitor will choose the action “Conduct Espionage”.

The competitor’s mixed strategy $(\alpha, 1 - \alpha)$ indicates that the competitor chooses the action “Conduct Espionage” and the action “Do Not Conduct” with a probability of $\alpha$ and $1 - \alpha$ respectively. Since a player chooses a mixed strategy when he/she is indifferent between alternative strategy choices because it yields the same payoff, the two rewards of the target are equated to obtain.

$$-(P_1 M + z_1)\alpha - z_1(1 - \alpha) = -(P_0 M + z_0)\alpha - z_0(1 - \alpha)$$

(2)

Rearranging yields

$$\alpha = \frac{z_1 - z_0}{M(P_0 - P_1)}$$

(3)

When the competitor chooses the above mixed strategy $(\alpha, 1 - \alpha)$, the target’s rewards from two action rewards are indifferent. Regardless of the target’s strategy, the total reward to the target will not change, because the competitor chooses the Nash Equilibrium.

The target’s mixed strategy $(\beta, 1 - \beta)$ indicates that the target chooses the action “Invest More” and the action “No Change” with a probability of $\beta$ and $1 - \beta$ respectively. Equating the two rewards results in

$$\beta(\mu P_1 M - Q_1) + (1 - \beta)(\mu P_0 M - Q_0) = \beta(0) + (1 - \beta)(0)$$

(4)
From the above equation, we get

\[ \beta = \frac{\mu P_0 M - Q_0}{\mu P_0 M - Q_0 - (\mu P_1 M - Q_1)} \]  

(5)

\[ L = \frac{P_0 z_1 - P_1 z_0}{P_0 - P_1} \]  

(6)

When \( z^* \leq z_0 < z_1 \), \( \mu P_1 M - Q_1 < 0 \) and \( \mu P_0 M - Q_0 < 0 \) The function \( PM + z \) has its minimum value with \( z = z^* \). When the probability that the competitor chooses the action “Do Not Conduct Espionage” is 100%, the target will choose the action “No Change” with 100%. There is no reason for the target to increase the investment to protect its trade secrets. The values of \( \alpha \) and \( \beta \) both equal 0. The expected reward to the competitor, \( H \), is 0. The expected reward to the target, \( L \), is \( -z_0 \). When we assume \( z_1 - z_0 = \varepsilon \) and \( \varepsilon \to 0 \), we can get a dynamic game model. \( -z^* \) is the minimum loss of the target.

With changes to the \( \mu \) value, the general sum static game model can represent different cyber espionage games in which competitors have different preferences.

To make our model simple, useful, and applicable, we have two assumptions.

1. The deterrence function is positively and linearly related to the investment on trade secret protection.
2. The industrial cyber espionage is a perfect information game.

For the general game, the following two propositions are supported by simulation results.

1. There is an optimal investment to minimize the target’s loss.
2. There is an optimal investment to minimize the reward to the competitor.

Furthermore, the model is validated by using simulations to prove three intuitive behavioral actions:

1. Given identical deterrence functions, a sensitive breach function can lead to a lower optimal trade secret protection investment than a less sensitive breach function.
2. Given identical breach functions, a high level deterrence function leads to a lower optimal trade secret protection investment than a low level deterrence function.
3. Given identical breach functions and deterrence levels, the more the utilization of trade secrets by a competitor, the greater is the optimal investment to protect it.

SIMULATION RESULTS AND DISCUSSIONS

Simulations were conducted in MatLab to demonstrate the behavioral actions. The discount rate \( \mu \) was described in Section 3. The discount rate \( \mu \) is also termed the utilization rate. Figure 1 demonstrates how the optimal investment on trade secret protection, from the target’s perspective, changes with breach functions with different sensitivities, different deterrence levels, and different utilization rates.

The first class of Gordon and Loeb’s breach function, with different parameter values for \( a \) and \( b \), \( P = \frac{1}{2z+1} \) and \( P = \frac{1}{(3z+1)^2} \) and Hausken’s breach function with different parameter values for \( \rho \)
and τ, $P = \frac{1}{1+0.0001(e^τ-1)}$ and $P = \frac{1}{1+0.0001(e^{2τ}-1)}$ are used for our simulation. The deterrence function is modeled as a simple linear relationship between deterrence and protection level with the assumption that when the protection investment increases, the deterrence to competitors increases. The deterrence function with two different parameter values used are, $Q = z$ and $Q = 5z + 5$. This allows us to compare the impact of investments on high and low deterrence levels. A total of 8 cases are analyzed. They are the combinations of two breach functions (Gordon and Loeb, and Hausken), their sensitiveness (sensitive and insensitive), and deterrence level (high and low). Table 2 present the implications of the parameter values. Two levels were used for each parameter: high and low. For each case, the utilization rate is changed from 0.05 to 1 with 0.05 increment to reflect the behavior utilization of trade secrets. The simulation results indicated very similar behavior for Gordon and Loeb’s and Hausken’s functions, and we only report on Gordon and Loeb’s breach function.

<table>
<thead>
<tr>
<th>Parameter Values</th>
<th>Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Utilization Rate (if $μ ≥ 0.9$)</td>
<td>The utilization rate of breached trade secrets is high</td>
</tr>
<tr>
<td>Low Utilization Rate (if $μ ≤ 0.1$)</td>
<td>The utilization rate of breached trade secrets is low</td>
</tr>
<tr>
<td>More Sensitive Breach Function</td>
<td>Trade secrets are well protected: Critical trade secrets</td>
</tr>
<tr>
<td>$P = \frac{1}{(3z + 1)^2}$</td>
<td></td>
</tr>
<tr>
<td>$P = \frac{1}{1 + 0.0001(e^{2z} - 1)}$</td>
<td></td>
</tr>
<tr>
<td>Less Sensitive Breach Function</td>
<td>Trade secrets are not well protected: unimportant trade secrets</td>
</tr>
<tr>
<td>$P = \frac{1}{2z + 1}$</td>
<td></td>
</tr>
<tr>
<td>$P = \frac{1}{1 + 0.00001(e^z - 1)}$</td>
<td></td>
</tr>
<tr>
<td>High Level Deterrence $Q=5z+5$</td>
<td>High costs for competitors to steal Information Systems successfully</td>
</tr>
<tr>
<td>Low Level Deterrence $Q=z$</td>
<td>Low costs for competitors to steal Information Systems successfully</td>
</tr>
</tbody>
</table>

Figure 1 represents the results of the 4 cases with Gordon & Loeb’s breach function format. This figure clearly shows how the breach function sensitivity, deterrence level, and the direction competition rates affect the optimal investment of trade protection systems. Given an identical breach function and deterrence level, preventing industrial cyber espionage from a competitor, who has a high trade secret utilization rate, requires more investments in trade secret protection. Given an identical breach function sensitivity and utilization rate, low level deterrence requires more investments on trade protection systems. Given an identical deterrence level and utilization rate, insensitive breach function requires more investments on trade secret protection.
Figure 2 represents the results of the 4 cases with Hausken breach function format. This figure also shows how the breach function sensitivity, deterrence level, and the trade secret utilization rates affect the optimal investment of trade protection systems. However, the impacts of the breach function sensitivity and deterrence level on optimal investments are different. Figure 2 shows that the impact of breach function sensitivity is higher than that of deterrence level on optimal investments, especially at high utilization rates. Figures 1&2 show that if the utilization of trade secrets is high, the target company needs to spend more on trade secret protection.
DISCUSSION AND CONCLUSION

If two companies are direct competitors, either one may have an intention to steal the opponent’s trade secrets. Cyber espionage is an efficient way to achieve that. Although the offense company, which launches industrial cyber espionage, may not directly attack the victim company by its cyber network or employees, the offense company could outsource this contract to a third-party company or group. The third-party company may directly recruit hackers or insiders to steal the trade secrets from the victim company. According to our research, any contracts involving trade secret intelligence are expensive. Those third-party companies or groups will have sufficient financial resources and intentions after they get the contract. They could adopt any methods to achieve their goals including cyber espionage. By outsourcing the contract, the offense company might release its liability and claim innocence, since they never notice what the third-party company has done. They may also claim that the contract clearly forbade any espionage activities, which may be used by the third-party company or group.

A company having plenty of valuable trade secrets can change its breach function sensitivity by improving its protection. It also can rely on state/federal governments to increase the deterrence level to some extent. However, it cannot influence its competitor’s preference, because the values of its trade secrets determine its opponents’ preferences.

The breach function sensitivity reflects the quality of a company’s trade secret protection. Compared with the deterrence level, the breach function sensitivity is almost totally controlled by the victim company itself. In other words, a small investment can result in a significant decrease in the breach probability. Companies can leave the job of increasing the deterrence level to legal frameworks. The role of the deterrence function is to reduce the competitor’s rewards by penalizing the competitor. All cyber espionage activities require effort and may result in negative
consequences. Our deterrence function incorporates the offense company's costs and the potential punishment.

Deterrence is a psychological process. Before an offense action taken by a competitor, it may consider the potential gain and loss. If the gain is much larger than the loss, the competitor will be tempted to commit cyber espionage. However, decision makers of different companies have different subjective evaluations of the gain and loss.

The contribution of this research is to combine economic theory, deterrence theory, and cyber security to explore the economic impact of industrial cyber espionage. The game theory research framework led to results that were intuitive and therefore this framework can help academics and practitioners understand cyber espionage and its economic impact. Companies that have more valuable trade secrets need to invest more heavily in trade secret protection than other companies. Federal and state governments also have a stake in protecting companies owning valuable trade secrets, by providing a deterrence framework within the legal system. In the future, we will design a dynamic game theoretical model to study cyber espionage in a further step.

References


