Optimal IS Security Investment: Cyber Terrorism vs. Common Hacking

Research-in-Progress

Introduction

Recently, many researchers have called paying more attention to cyber terrorism (Foltz, 2004; Estevez-Tapiador, 2004; Embar-Seddon, 2002). Park and Duggan (2001) have defined cyber terrorism as a new approach adopted by terrorists to attack cyberspace and an extension of traditional terrorism. The threat of cyber terrorism is more dangerous than that of common IS attacks launched by common hackers (Rogers, 1999; Verton, 2003). IS security and cyber terrorism are no longer just the concern of national and state governments. Organizations that compose the critical infrastructure of national economy should be very careful about the potential attacks from terrorism (Nickolov, 2005). Information systems of critical infrastructure includes the servers, databases, networks, routers and all other important components making up the information network such as Internet, private networks, and all public and private networks and systems facilitating information sharing, processing, storing, analyzing, and collection.

Cyber terrorists belong to the communities of terrorists and hackers, and inherit characteristics of both terrorists and hackers. Moreover, cyber terrorists are a subgroup of terrorists and also a subgroup of hackers. One possible way to differentiate cyber terrorism from traditional hacking and other cyber crime is by ascertaining the motivation or intention of the person or group launching the attack (Embar-Seddon, 2002). The motivation of cyber terrorists are driven by political or religious doctrines. They create fear and panic among civilians or disrupt or destroy public and private infrastructures. They wish to push the target government to negotiate with them, or wish to show their existence to their community, or their political and financial supporters (Embar-Seddon, 2002; Verton, 2003). Hackers can be either cyber terrorists or common hackers. Common hackers' motivations include compulsion to hack, curiosity, intention to gain power, peer recognition and belonging to a group (Beveren, 2001). Thus, the difference in the motivation of cyber terrorists and common hackers suggests that the models for analyzing common hackers' threats, for organizations, may be different than for cyber terrorists. Throughout our discussions, organizations refer to both government agencies and private companies.

The quality of IS security is highly related to the investments in IS security (Bojanc and Jerman-Blazic, 2008). The appropriate level of IS security investment can enhance the capability of organizations and governments to defend attacks launched by the most dangerous hacker group, namely cyber terrorists (Bodin and Gordon, 2005). The objective of IS security is to minimize an organization's potential losses by balancing the investment cost and financial losses from intrusions. A solid theoretical foundation concerning risk analysis and cyber terrorists' behavior prediction has not been well established in the field of IS security. Without proper risk and behavioral analysis, non-optimal investment decisions in IS security will be made both in organizational and critical infrastructure security systems. If organizations are investing only to protect themselves against common hackers, that investment may not be enough to protect themselves from attacks from cyber terrorists.

The aim of this paper is to utilize game theory to analyze risks in information systems and predict the behavior of cyber terrorists and common hackers. Our goal in this paper is to compare the optimal investment decision for organizations to protect themselves from common hackers and from cyber terrorists. The main contribution of this paper is that a two-stage stochastic game model has been proposed and the model can be applied to all cyber crimes including cyber terrorism activities as well as common hacking activities.

Background

Prevention of cyber-crime involves the study of IS security research and implementation techniques. Research on IS security provides an understanding of the methods, threats, risks, and behavioral aspects of cyber crimes. Currently, there are three streams of research related to IS security: technology-based

(Lee et al, 2002; Denning and Branstad 1996; Sandhu, et al, 1996), behavioral based (Fahnot, 2007; Workman and Gathegi, 2007; Rogers, 2001; Kjaerland, 2005; Skinner and Fream, 1997), and economic based (Finne, 2002; Hoo, 2000; Meadows, 2001; Gordon et al, 2003; Varian, 2002; Campbell et al., 2003; Garg et al, 2003, Ettredge and Richardson, 2002). This paper presents literature on the behavioral and economic perspectives of IS security research and provides adequate background on cyber terrorists to compare them with common hackers. Another stream of research on deterrence theories is critical to this work since the deterrence levels for hackers and cyber terrorists are different.

Cyber Terrorism

The word "Terrorism" can be traced back to the French Revolution when terror was used by the government to suppress counter-revolutionary adversaries (Harzenski, 2003). Most terrorists share two common aspects: (1) they assault civilians; (2) they target victims that are not their true targets, but these victims do influence the target audience. Terrorists rely on terrorism and low intensive conflict to erode the enemy's moral and physical capacities (Opprea and Mesnita, 2005). Victoroff (2005) proposed a comprehensive typology to illustrate the dimensions of terrorism. The demographic data about terrorists have been presented in the studies by Hassan (2001), Pedahzur et al. (2003), and Sageman (2004).

The literature review on terrorism indicates that some terrorists are highly educated and may even obtain financial support for their actions. Since the late 1990s, Middle East terrorists have come from a wide demographic range, including university students, professionals, and young women (Rees, 2002). According to recent research, most terrorists come from a middle class background (Hassan, 2001; Pedahzur et al., 2003; Sageman, 2004) and have professional backgrounds (Krueger and Maleckova 2003, Sageman 2004). Thus, it is reasonable to assume that many terrorists are highly educated and are computer literate and therefore may employ cyber terrorist activities.

Cyber terrorists only can be differentiated from the other hacker groups by their attack motives (Embar-Seddon, 2002). All cyber attack methods adopted by cyber terrorists are the same as those adopted by the other hacker groups. Cyber terrorists can launch DDOS attacks to disrupt servers, or intrude into public media systems to spread rumor or alert civilian targets. Although cyber terrorists cannot cause death on a large scale like physical terrorism incidents, their actions might result in large monetary losses exceeding that of physical terrorism. With adequate financial resources, cyber terrorists, requiring fewer inputs, can hide their identities and use sophisticated technical attacks remotely in a concerted manner. This level of financial resources and planning is not in the purview of common hackers and the level of motivation guided by core beliefs is also absent for common hackers (Warren, 2007).

IS Security Investment

Bojanc and Jerman-Blazic (2008) presented an approach towards assessing the required information and communication technology (ICT) security investment and data protection through the identification of assets and vulnerabilities. Huang et al. (2008) modeled the decision-maker of an organization as risk-averse, and adopted the expected utility theory to determine the optimal security investment level. Liu et al. (2008) empirical analysis based on a survey of Japanese firms, revealed that the effects of the information security investment were to reduce the vulnerability effects.

Gordon and Loeb (2002) believed that previous studies related to the economic aspects of information security provided little generic guidance on how to derive a proper amount to invest in IS security. Hence, they built a model that considered how the vulnerability of information and the potential loss from such vulnerability affected the optimal funding to secure that information. Hausken (2006) proposed new logistic breach functions to address some of the drawbacks of the Gordon and Loeb's breach function.

Schechter and Smith (2003) used game theory to develop a model for companies to gauge their attractiveness to thieves and determine the proper level of security required for packaged systems. Their research revealed that a company would benefit substantially by increasing the probability of detection and/or the probability of repelling the attack, and by increasing the likelihood of hacker convictions. Cavusoglu (2003) used game theory to analyze the value of Intrusion Detection Systems (IDS) within an IT network that has firewalls on one side and manual monitoring on the other hand. Cavusoglu et al (2008) compared game theory and decision theory approaches on the investment levels, vulnerability, and payoffs from investment. The paper clearly claimed that game theory was appropriate to model IS security investment. Garcia and Horowitz (2007) constructed a Markov Perfect Equilibrium game-theoretical model to explore the economic motivations for investment in added Internet security.

The Deterrence Function in IS security

Straub and Welke (1998) considered deterrence theory as a theoretical basis for security countermeasures to reduce IS risks. Their research highlights the influence of managerial policies for deterrence, prevention, detection, and recovery from cyber threats, which may have a similar impact on cyber terrorism.

Deterrence theory has been widely employed in the fields of economics and criminology to study the behavior of criminals and antisocialists (Becker, 1968; Pearson and Weiner, 1985). In criminology, deterrence theory focuses on the effects of punishment. Deterrence theory, in this field, 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 and Weiner, 1985). In economics, deterrence theory focuses on the reward of legal behavior and the punishment of illegal behavior (Becker, 1968). To deter potential criminals from committing unlawful behavior, it is necessary to impose countermeasures that increase the cost, and or reduce the benefits, associated with doing so (Becker, 1968). Thus, from both the criminology and the economics deterrence theories, we can posit that, for cyber terrorism, the expected punishment depends upon the legal national and international framework, and the perceived probability of being caught depends upon the ability to identify the perpetrators and the cooperation for information sharing between nations. These frameworks are only in the nascent stages and international cooperation to prosecute criminal activities will only work if the two nations are signatories of a convention. Moreover, deterrence based on identification of cyber terrorists is difficult because technical means are available to hide their footprints as discussed in the previous section. Wible (2003) proposed two approaches to deter cyber hackers: (1) reinforce the criminal law and increase punishment, and (2) the least dangerous kinds of hacking should be decriminalized in ways that demarginalize the hacking community. Workman and Gathegi (2007) found that punishment and ethics education are effective in deterring cyber criminal behavior. Oksanen and Valimaki (2007) found that the classic deterrence model should incorporate the reputational cost of violations and the reputational benefit of violations. Based on their research, we can posit that the existence of the reputational benefits behind cyber terrorism may exist. The increased reputation from peer groups after a successful cyber attack may motivate cyber terrorists to advertise their activities.

Becker (1968), in his classical paper about punishment determination, believed that punishment determination has to consider the social cost of punishments and that all punishments can be converted to monetary values. Legal systems in most societies specify punishments that increase with the level of social harm caused by the criminal activities (Rasmusen, 1995). As cyber terrorism becomes more harmful, based on Becker's theory, increasing the punishment substantially for the sake of the additional deterrence may be worth the costs, however, it is difficult to quantify the level of punishment that will stop cyber terrorism.

Methodology

Game theory is a branch of applied mathematics widely applied in economics, accounting, finance, biology, and political science. Game theory has numerous applications, ranging from solving problems involving offense and defense (Cavusoglu, 2003; Lye and Wing, 2005; Sallhammar et al., 2007) to the design of optimal penalties to deter crime, which can be viewed as a rational choice decision (Saha and Poole, 2000; Chu et al, 2000). Their paper described how game theory can be used to find strategies for both an attacker and the administrator. In the game theory, the Nash equilibrium is a methodology used in non-cooperative games whereby no player can gain more by changing his/her strategy unilaterally (Brams, 1992). In game theory, pure strategies specify the nonrandom action selection of players. Contrary to pure strategies, mixed strategies specify the set of actions from which a random selection will be made. For example, if a cyber terrorist has an action set {Attack, Do Not Attack}, a mixed strategy of (30%, 70%) will result in selecting the action "Attack" with a probability of 30 percent and the action " Do Not Attack" with a probability with 70 percent, respectively.

Formally, a two-player stochastic game consists of $(S, A^1, A^2, P, R^1, R^2, \omega)$, where

- S= { S_1, S_2, …, S_N} is the state set with Markov chain property. N denotes the maximum number of state in the stochastic game.
- A^k ={ a_1^k, a_2^k, $a_{3,\ldots\ldots,}^k a_N^k$} k=1,2, is the action set of player k, and N= the maximum state number
- $P = P(s'|s,a^1,a^2)$, where s, and $s' \in S = \{S_1, S_2, S_3, S_4, \ldots S_N\}$, is state transition probability from state s to state s', with player 1 choosing a^1 and player 2 choosing a^2.
- R^k: k=1, 2, is the reward function of player k.
- ω: [0,1]is the discount parameter for discounting future rewards.

A state transition has a reward worth its full value, but the reward for the transition to the next state is worth only ω multiplied by its value at the current state. The discount factor, ω, represents the importance of future rewards to a game player. A high discount factor means a player cares more about rewards in the future. With a high discount factor, a hacker has a long term objective to intrude into the information system. Thus, for cyber terrorists, we set ω to a high value. A low discount factor means that he/she only cares about the rewards in the near future, which is true for common hackers.

The rules of the game are as follows. At a discrete time t, the game is in state $S_t = s \in S$. Examples of actions for the state are: Player 1 chooses an action a^1 from A^1, and Player 2 chooses an action a^2 from A^2. Player 1 will receive a reward $R^1(s, a^1, a^2)$, and player 2 will receive a reward $R^2(s, a^1, a^2)$. When $S_{t+1} = s'$, the game moves from the current state $S_t = s$ to the next state $S_{t+1} = s'$ with conditional probability P (s' | s, a_t^1, a_t^2). Player 1 will receive a reward $R^1(s')$, and player 2 will receive a reward $R^2(s')$. $v_\varphi^k(s')$ is the expected discounted reward to player k at the state s'.

$$R^k(s, v_\varphi) = [r^k(s, a^1, a^2) + \varphi \sum_{s' \in S} p(s'|s, a^1, a^2) v_\varphi^k(s')]$$

In this research, a 2-stage stochastic game model is developed to predict and analyze the behavior of a hacker group and a targeted organization in an IS security game. Because cyber terrorists are a subgroup of hackers, this model can be applied to cyber terrorism as well as common hacking. To make our research sound, we have three assumptions.

1. The first assumption: The targeted information systems are not valuable to common hackers, but valuable to cyber terrorists.
2. The second assumption: The deterrence function is positively and linearly related with the security investment.
3. The third assumption: Hackers know what kind of actions will trigger IDS Alarms.

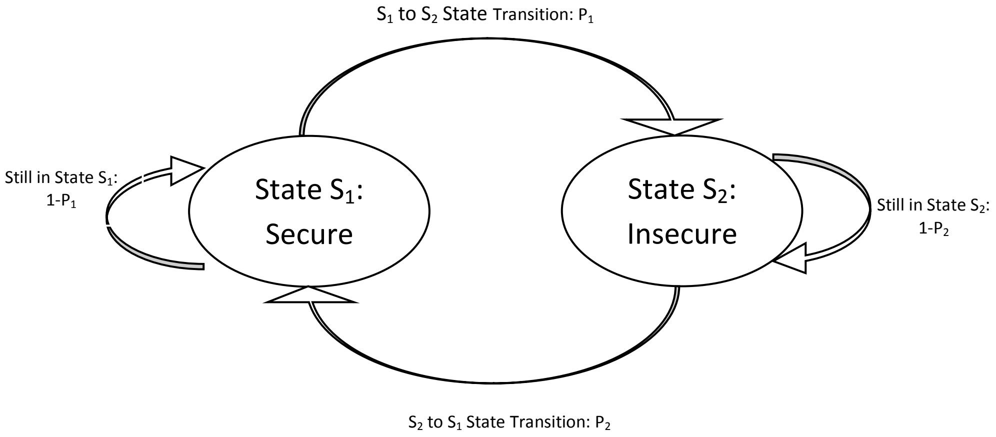

S$_1$ to S$_2$ State Transition: P$_1$
Still in State S$_1$: 1-P$_1$
State S$_1$: Secure
State S$_2$: Insecure
Still in State S$_2$: 1-P$_2$
S$_2$ to S$_1$ State Transition: P$_2$

Figure 1 State Transition

Two (2) states and two (2) action sets are used to analyze the behaviors. The state transition process is illustrated in Figure 1. There are two states in this game: the secure state and the insecure state. P_1 represents the probability that a hacker successfully breaches the system, thereby intruding upon the information system. P_2 represents the probability that the hacker is detected by the intrusion detection system after a successful intrusion. The game initially starts from the secure state. With a probability of P_1, the information system will transfer to the insecure state. Once the information system is in the insecure state, with a probability of P_2, the information system will transfer back to the secure state.

Figures 2 and 3 present this general sum stochastic game. In this game, without extra investment in preventive control, the probability that a hacker successfully intrudes upon the information system is given by P_1^0. The superscript zero (0) represents the initial investment. When the target invests more in preventive control, the probability that the hacker successfully intrudes upon the information system is given by P_1. The notation is similar for the Intrusion Detection Systems (IDS). The state transition probability P_1 is equal to the breach function P(z), where z is the investment. The state transition probability is P_2, while P_2^0 represents the IDS detection rate.

Secure State
Target Organization

		Invest More In Preventive control	Do Not Invest More In Preventive control
Hacker	Intrude	(r_1^1, r_1^2) $(1-P_1,P_1)$	(r_2^1, r_2^2) $(1-P_1^0, P_1^0)$
	Do Not Intrude	(r_3^1, r_3^2) $(1,0)$	(r_4^1, r_4^2) $(1,0)$

Figure 2 Rewards to two players in the secure state

Insecure State
Target Organization

		Invest More In IDS	Do Not Invest More In IDS
Hacker	Violate	(R_1^1, R_1^2) $(P_2, 1-P_2)$	(R_2^1, R_2^2) $(P_2^0, 1-P_2^0)$
	Do Not Violate	(R_3^1, R_3^2) $(0,1)$	$(R_4^1, -R_4^2)$ $(0,1)$

Figure 3 Rewards to two players in the insecure state

In the secure state, the hacker has his/her action set {Intrude, Do Not Intrude}, while the target has its action set {Invest More in Preventive Control, Do Not Invest More In Preventive Control}. Preventive control includes the implementation of security mechanisms, such as firewalls, access control, antivirus, social engineering education and other managerial practices, logging, and cryptology.

The two-stage stochastic game model captures different aspects of a security game. In the secure stage, the organization is faced with the task of investing more in preventive control. As an example, when an organization detects a social engineering attack, the organization can alert (invest more) the employees on safeguarding against social engineering attacks. These decisions are available to the organization for each of the preventive control mechanisms. According to the characteristics of stochastic games, the stages transit randomly with probabilities. Hackers know the stages, while targeted organizations may not know until they find some clues. Organizations must allocate their security investment properly in their preventive control and detective control.

In the insecure state, the hacker has his/her action set {Violate, Do Not Violate}, while the targeted organization has its action set {Invest More In IDS, Do Not Invest More In IDS}. According to the working principles of the IDS, when a hacker is able to foil the IDS, the hacker remains undetected by the IDS, i.e., the hacker was successful in violating the internal network security policies. The hacker may browse important files, or just listen to the network traffic. This phenomenon is modeled as the “Violate” action. In contrast, if the IDS system is able to detect an intrusion, the intruder is immediately shut off from listening to the network. It is possible that an intruder, while violating the IS security policy, triggers a rule that leads to the IDS detecting the violation, thereby closing off access to the intruder. A detailed explanation about the payoffs in the insecure state is given as request.

The respective payoffs as given by $r_{1,2}$ and $R_{1,2}$ in the Secure or Insecure state are breach/detection functions of P(z), the investment level (z), the maximum payoff (M), a discount rate (ω), and a deterrence function D(z). The deterrence function is modeled as an increasing monotonic function of the investment level as posited by the criminology theory of deterrence e.g, a society that expends greater resources in systems (prisons and legal systems) to punish criminal activities will have a greater deterrence effect on subsequent criminal activities. The discount rate is reflective of the amount of effort and planning expended to breaching the system. A low discount rate (ω) is reflective of common hackers who without any planning are fishing in the dark for information and their fingerprints within the network can be traced easily to effectively shut them down soon. In contrast, a high discount rate reflects cyber terrorists who have ample knowledge and resources to plan out an attack with a great degree of sophistication. We model a typical payoff in the Secure or Insecure state such as $\Gamma_{\mathrm{s}}^{\mathrm{k}} = r_s^k + \omega[(1 - P_s)\Gamma_{\mathrm{s}}^{\mathrm{k}} + P_s\Gamma_{\mathrm{s'}}^{\mathrm{k}}]$, where $\Gamma_{\mathrm{s}}^{\mathrm{k}}$ represent k player’s reward at s stage and ω represents hackers’ preference (discount rate).

Cyber terrorists intrude and breach the organizations’ information systems not for monetary gains but to create chaos to influence civilian audiences. Common hackers usually work for money. Most targets aimed by cyber terrorists are not valuable for common hackers. Common hackers won’t hold a long term goal for these targets. We can use a discount factor to differentiate common hackers from cyber terrorists. Moreover, another parameter that we address is the breach function sensitivity. Assets that need to be protected will be guarded more effectively. The third aspect that we address is the deterrence level. Thus, the discount factor is only one of the many measures that capture the differences between hackers and cyber terrorists.

Terrorists have been known to sacrifice their lives and have considerable more resources at their disposal. Therefore, relatively speaking, cyber terrorists will exert a lot more effort than common hackers who may not have the network support and financial resources to launch a very sophisticated attack against highly protected systems. Common hackers won’t have a long term goal for these highly protected targets.

The deterrence function’s role is used to balance the hackers’ logic reasoning. All hacking works require certain efforts and may result in some negative consequences. Our deterrence function incorporates hacker’s efforts and potential punishment. It is well known that terrorists are willing to sacrifice their lives to inflict damage to the target and the deterrence function captures that much higher deterrence level to thwart cyber terrorists compared to common hackers.

The stochastic game is dynamic. Initially, the states transit without any clues until the whole game reaches a steady state, in which both of players find their optimal rewards and equilibrium. If a hacker successfully intrudes an information system and browses the system just like an employee, it would be very difficult for the IDS to find this hacker. If the hacker participates in hostile acts, the IDS could find the hacker.

The stochastic game was solved with the non-linear programming function in MatLab software. Simulations were conducted in MatLab to compare the behavior of hackers and cyber-terrorists and to identify the optimal investment to secure information systems. Two parameters: the discount rate, and the deterrence level were varied for the simulation runs. The simulations were repeated on two different breach functions to analyze the robustness of the results: Gordon and Loeb’s breach function $\frac{1}{(\mathrm{az}+1)^{\mathrm{b}}}$, and Hausken’s breach function $\frac{1}{1+\mathrm{a}(\mathrm{e}^{\mathrm{bz}}-1)}$ with changes to the parameters. In both cases, the parameters a and b were selected so as to make the breach function very sensitive to investments i.e., we assume that the organization has diligently tried to avoid breaches by sound management policies. The investment amount was changed from 1% of the maximum loss to 15% of the maximum loss for each simulation run. Table 1 presents the implications of the parameter values used in the simulation, respectively. Two levels were used for each parameter: high, and low. Because the non-linear stochastic game optimization can lead to non-optimal solutions, each simulation began from different starting criteria. In total, 100 simulations were carried out for each combination of the parameter values.

Table 1 The Implication of the Parameter Values

Parameter Values		Implications
High Discount rate	$\omega = 0.9$	Cyber Terrorism Attacks
Low Discount rate	$\omega = 0.1$	Common Hacker Attacks
High Deterrence Level	Q=4z	High costs to hackers to intrude or Organizations have abilities to trace, capture and sue attackers
Low Deterrence Level	Q=z	Low costs to hackers to intrude or Organizations have few abilities to trace, capture and sue attackers

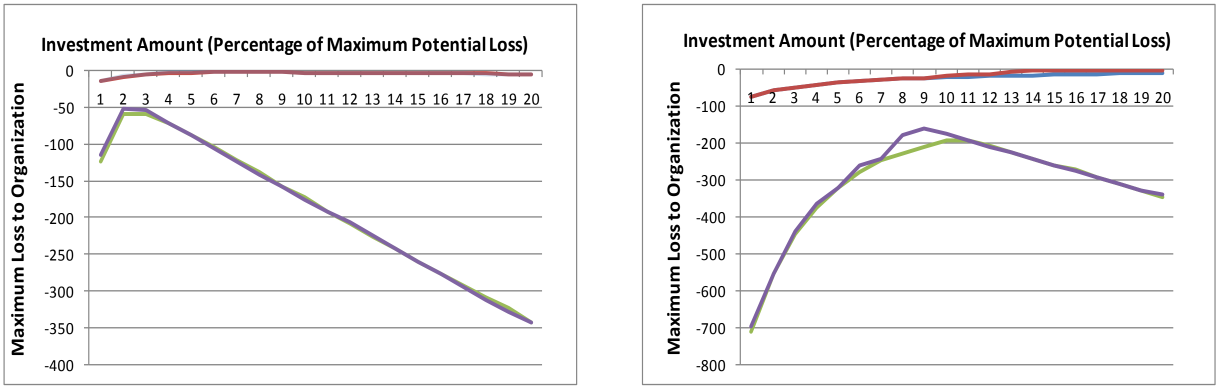
The total maximum loss to the target was determined for each simulation. The total maximum loss was the sum of the loss to the target in the secure state and the insecure state. The average value for the total maximum loss was calculated from the 100 simulations, in which the parameter values were the same. The detail simulation is upon the request.

Table 2 Breach Functions

	Gordon and Loeb's Function Format	Hausken' s Function Format
Sensitive Breach Function	$P = \frac{1}{(2z+1)^2}$	$P = \frac{1}{1+0.001(e^{2z}-1)}$
Insensitive Breach Function	$P = \frac{1}{z+1}$	$P = \frac{1}{1+0.0001(e^{z}-1)}$

Figure 4 compares the maximum amount of loss to an organization for cyber terrorist and common hackers with varying organizational investment levels. Figure 4 totally incorporates 8 different conditions: 2 different deterrence levels, 2 different sensitive breach functions, and 2 different discount rates. Due to the page limit, Figure 4 didn't include the results from Hausken's breach function format. However, the final outcome from Hausken's breach function format is the same as that from Gordon and Loeb's breach function format.

The maximum loss includes the investment that the organization needs to invest in, to protect its resources, and losses due to the breaching activity. Figures 4(a) and 4(b) depict the results for Gordon and Loeb's breach function format. In Figures 4(a) and 4(b), green lines represent the conditions with a high discount rate, a low deterrence level and a sensitive breach function; purple lines represent the conditions with a high discount rate, a high deterrence level and a sensitive breach function; red lines represent the condition with a low discount rate, a high deterrence level and a sensitive breach function; blue lines represent the condition with a low discount rate, a low deterrence level and a sensitive breach function. In Figure 4, blue and red lines represent common hackers, and green and purple lines present cyber terrorists. Two results are evident from Figure 4: 1) there is an optimal investment level that minimizes the maximum loss to the organization, and 2) the maximum loss to the organization is far much less for common hacker attacks than for cyber terrorist attacks. While, the figure does not depict the degree of the maximum loss, our simulated data indicates that the maximum loss for cyber terrorists is significantly more than for common hackers. Considering that both the cyber terrorist and the hacker rely on the same tool sets to attack an organization's networks, these results reveal that the maximum loss to the organization depend upon other factors: deterrence level and the planning level of the attacker. This result is not surprising due to the fact that the attack motive for cyber terrorists is far more different than for common hackers.



4(a) 4(b)

Figure 4. Comparison of Maximum Loss to Organization for Cyber Terrorists and Common Hackers

Conclusion

Using a game theoretical model, we propose and prove that cyber terrorist attacks can lead to far greater losses to an organization than a common hacker attack. We also show that an optimal investment exists for games such as cyber crimes. To the best of our knowledge, our approach is a novel approach that combines economic theory, deterrence theory, and IS security to explore the cyber terrorism problem.

Organizations are facing the challenge of improving IS security, as well as minimizing IS security expenses. Increasing investment in IS security may not be justified based on the marginal benefits of the investment. Two similar companies may spend an equal amount on securing their information systems, but the level of security achieved may be quite different. IS security does not depend on the investment amount only. In this paper, we claimed that, in addition to the investment amount, two variables, namely, the hackers' preference (Discount Rate), and the deterrence level, affect the optimal investment for IS security. The discount rate represents a hacker's preference. The simulation results of our game model prove that the hackers' preference and the deterrence level have an effect on the optimal investment. When we applied the model to explore cyber terrorism, we can find that with increasing discount rate, the optimal investment will increase. The threat of cyber terrorism will force organizations to spend more money to safeguard their information systems. Either market driven forces (when an attack cripples an organization), or regulatory mandates can lead to such increased spending for organizations.

This research can also be generalized to other practical fields such as financial fraud prevention. If we view inside employees as potential cyber criminals, this game model will tell us that building a strong internal control system is as important as increasing deterrence level. Internal fraud from employees who can have a long-range goal for fraudulent activity could be more dangerous than actions originating from other employees.

Reference

Becker, S. G. 1968. "Crime and punishment: An economic approach," *Journal of Politic Economy*(76:2), pp. 167-217.

Beveren, J. V. 2001. "A conceptual model of hacker development and motivations," *Journal of E-business* (1:2), pp. 1-9.

Bodin, L. D., and Gordon, L. A. 2005. "Evaluating information security investments using the analytic hierarchy process," *Communication of ACM* (48:2), pp. 79-83.

Bojanc, R. and Jerman-Blazic, B. 2008. "Towards a standard approach for quantifying an ICT security investment," *Computer Standards & Interfaces* (30), pp. 216-222.

Brams, S. J. 1992. "Game theory and literature," *Games and Economic Behavior* (6:1), pp. 32-54.

Campbell, K., Gordon, L.A., Loeb, M. P., & Zhou, L. 2003. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security*, (11:3), pp. 431–448.

Cavusoglu, H. 2003. The economics of information technology security. Doctoral Dissertation, University of Texas at Dallas, Texas, USA.

Cavusoglu, H., Raghunathan, S., and Yue, W. T. 2008. "Decision-theoretical and game-theoretical approaches to IT security investment," *Journal of Management Information Systems* (25:2), pp. 281-304.

Chu, C.Y. C., Hu, S., and Huang, T. 2000. "Punishing repeat offenders more severely," *International Review of Law and Economics* (20:1), pp. 127-140.

Denning, D., and Branstad, D. 1996. "A taxonomy of key escrow encryption systems," *Communications of the ACM* (39:3), pp. 34-40.

Embar-Seddon, A. 2002. "Cyberterrorism," *American Behavioral Scientist* (45:6), pp.1033-1043.

Estevez-Tapiador, J.M. 2004. "The emergence of cyber-terrorism," *Computer Society* (5:10), pp. 1-3.

Ettredge, M. and Richardson,V.J. 2002. "Assessing the risk in E-Commerce," in *Proceedings of the 35th Hawaii International Conference on System Sciences*, Big Island, Hawaii: IEEE Computer Security, pp. 194-204.

Fahnot, I.J. 2007. "Behavioral information security," In L.J. Janczewski, Cyber warfare and cyber terrorism, Idea Group Inc (IGI).

Finne, T. 2002. "A conceptual framework for information security management," *Computer & Security* (17:4), pp. 303-307.

Foltz, C.B. 2004. "Cyberterrorism, computer crime, and reality," *Information Management & Computer Security* (12: 2/3), pp. 154-166.

Garcia, A. and Horowitz, B. 2007. "The potential for underinvestment in internet security: implications for regulatory policy," *Journal of Regulatory Economics* (31:1), pp. 37-55.

Garg, A., Curtis, J., and Halper, H. 2003. "The financial impact of IT security breaches: What do investors think?" *IS security* (12:1), pp. 22-33.

Gordon, L. A., and Loeb, M. P. 2002. "The economics of information security investment," *ACM Transactions on Information and System Security* (5:4), pp. 438-457.

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. 2003. "Sharing information on computer systems security: an economic analysis," *Journal of Accounting and Public Policy* (22:6), pp. 461-485.

Harzenski, S. 2003. "Terrorism, a History: Stage One," *Journal of Transnational Law & Policy* (12:2), pp. 137-196.

Hassan, N. 2001. "An arsenal of believers: Talking to the human bombs," *The New Yorker*, November 19, 2001.

Hausken, K. 2006. "Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability," *Information System Front* (8:5), pp. 339-349.

Hoo, K. J. S. 2000. How much security is enough: A risk management approach to computer security. Doctoral Dissertation, Stanford University, Stanford, CA, USA.

Huang, C. D., Hu, Q., and Behara, R. S. 2008. "An economic analysis of the optimal information security investment in the case of a risk-averse firm," *International journal of Production Economics* (114:2), pp. 793-804.

Kjaerland, M. 2005. "A classification of computer security incidents based on reported attack data," *Journal of Investigative Psychology and Offender Profiling* (2:2), pp.105 – 120.

Krueger, A. and Maleckova, J. 2003. “Education, poverty, political violence, and terrorism: Is there a connection?” *Journal of Economic Perspectives* (17:4), pp. 119-144.

Lee, W., Fan, W., Miller, M., Stolfo, S. J., and Zadok,E. 2002. “Towards cost-sensitive modeling for intrusion detection and response,” *Journal of Computer Security* (10:1-2), pp. 5-22.

Liu, W., Tanaka, H., and Matsuura, K. 2008. “Empirical analysis methodology for information-security investment and its application to reliable survey of Japanese firms,” *Information and Media Technologies* (3:2), pp. 464-478.

Lye, K., and Wing, J.M. 2005. “Game strategies in network security,” *International Journal of Information Security* (4:1-2), pp. 71-86.

Meadows, C. 2001. “A cost-based framework for analysis of denial of service in networks,” *Journal of Computer Security* (9:1/2), pp. 143 – 164.

Nickolov, E. 2005, “Critical information infrastructure protection: Analysis, evaluation and expectations,” *Information & Security* (17), pp. 105-119.

Oksanen, V., and Valimaki, M. 2007. “Theory of deterrence and individual behavior. Can lawsuits control file sharing on the Internet?” *Review of Law and & Economics* (3:3), pp. 693-714.

Oprea, D. and Mesnita, G. 2005 The Information System and the Global Terrorism (July - August 2005). Available at SSRN: http://ssrn.com/abstract=906289.

Parks, R. C. and Duggan, D. P. 2001. “Principle of cyber-warfare,” in *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, West point, NY, 5-6 June, 2001.

Pearson, F. S., and Weiner, N. A. 1985. “Toward an integration of criminological theories,” *Journal of Criminal Law and Criminology* (76:1), pp. 116-150.

Pedahzur,A., Perliger, A. and Weinberg, L. 2003. “Altruism and fatalism: The characteristics of Palestinian suicide terrorists,” *Deviant Behavior* (24:4), pp. 405- 423.

Rasmusen, E. 1995. “How optimal penalties change with the amount of harm,” *International Review of Law and Economics* (15:1), pp. 101-108.

Rees, M. 2002. “Why suicide bombing is now all the rage,” *Time*, April 15, pp. 9-33.

Rogers, M. 1999. “Psychology of computer criminals,” in *Proceedings of The annual Computer Security Institute Conference*, St. Louis, Missouri.

Rogers, M. 2001. A social learning theory and moral disengagement analysis of criminal computer behavior: an exploratory study. Doctoral Dissertation, University of Manitoba, Winnipeg, Manitoba.

Sageman, M. 2004. *Understanding terror networks*. Philadelphia: University of Pennsylvania Press.

Saha, A. and Poole, G. 2000. “The economics of crime and punishment: An analysis of optimal penalty,” *Economics Letters* (68:2), pp. 191-196.

Sallhammar, K., Helvik, B.E., and Knapskog S.J. 2007. “A framework for predicting security and dependability measures in real-time,” *International Journal of Computer Science and Network Security* (7:3), pp. 169-183.

Sandhu, R., Coyne, E., Feinstein, H., and Youman, C. 1996. “Role based access control models,” IEEE *Computing* (29:2), pp. 38-47.

Schechter, S. E., and Smith, M. D. 2003. “How much security is enough to stop a thief? The economics of outsider theft via computer systems networks,” in *Proceedings of the 7th Financial Cryptography Conference*, Guadeloupe, French: the International Financial Cryptography Association, pp. 122-137.

Skinner, W. and Fream, A. 1997. “A social learning theory analysis of computer crime among college students,” *Journal of Research in Crime and Delinquency* (34), pp. 495-518.

Straub, D. W., and Welke, R. J. 1998. “Coping with systems risk: Security planning models for management decision making,” *MIS Quarterly* (22:4), pp. 441-469.

Sunstein, C. 2003. *Why societies need dissent*. Cambridge: Harvard University Press.

Varian, H. 2002. “System reliability and free riding,” in *Proceedings of Workshop on Economics and Information Security*, University of California, Berkeley, May 16-17, 2002.

Verton, D. 2003. *Black ice: The invisible threat of cyber-terrorism*. McGraw Osborne Media.

Victoroff, J. 2005. “The mind of terrorist: A review and critique of psychological approach,” *The Journal of Conflict Resolution* (49:1), pp. 3-41.

Wang, J., Chaudhury, A., and Rao, H. R. 2008. “A value-at-risk approach to information security investment,” *Information Systems Research* (19:1), pp. 106-120.

Warren, J. 2007. “Terrorism and the Internet,” in *Cyber warfare and cyber terrorism*. L. J. Janczewski and A. M. Colarik (Eds). Chapter VI, pp 42-49,IGI Global.

Wible, B. 2003. “A Site Where Hackers Are Welcome: Using Hack-In Contests To Shape Preferences and Deter Computer Crime,” *The Yale Law Journal* (112:6), pp. 1577-1623.

Workman, M., and Gathegi, J. 2007. "Punishment and ethics deterrents: A study of insider security contravention," *Journal of the American Society for information science and technology* (58:2), pp. 212-222.