CERIAS Tech Report 2003-38

ESSAYS IN INFORMATION SECURITY

by Mukul Gupta

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

ESSAYS IN INFORMATION SECURITY

A Thesis

Submitted to the Faculty

of

Purdue University

by

Mukul Gupta

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

December 2003

Dedicated to
all the teachers in my life
especially my parents
and my sister

ACKNOWLEDGEMENTS

I would like to extend my gratitude to Prof. Alok Chaturvedi who has been my mentor and guru during my stay at Purdue. His guidance, ideas, constructive criticism, and inspiration were invaluable to my research as well as my professional development. I would also like to thank Prof. Shailendra Mehta for spending numerous hours providing me with guidance and encouragement through some difficult phases in my research. I am also indebted to Prof. Jackie Rees for being there for me whenever I needed support and for her constructive comments on my research. I am also thankful to Prof. Kemal Altinkemer for his guidance and support. I also appreciate Prof. Christopher Clifton for his ideas and comments on my dissertation.

I am grateful to Ms. Kelly Felty and the staff of doctoral programs office for their help and making my life comfortable during my stay at Purdue. I am also thankful to PERC (Purdue E-Business Research Center) and CERIAS (Center for Education and Research in Information Assurance and Security) for their financial support. I am also indebted to Mr. Midhilesh Mulpuri for providing excellent programming support for my research and being a constant critic of my design specifications. I am grateful to Jie Chi for his ideas on my research. I thank Chih-hui Hsieh and all other programmers at SEAS (Synthetic Economies for Analysis and Simulation) labs for their constant support for my project.

A special thank goes to Prof. Shivraj Kanungo, without whose encouragement, I would not have embarked on the path of doctoral studies. I am also thankful to my friends, Anjali, Ashutosh, Bonnie, Geetanjali, Hrishi, Kumar, Natasa, Rohit, Sami, Sanjay, Vivek and Wei for their constant encouragement. Most importantly I would like to thank my parents and sister for their love, encouragement, patience and support throughout my life.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Gupta, Mukul, Ph.D., Purdue University. December 2003. Essays in Information Security. Major Professor: Alok R. Chaturvedi.

Information Technology has become integral to organizations' pursuit to achieve a competitive edge in an interconnected environment. The information technology resources of organizations have become targets of perpetrators, who seek gains from causing damage to information resources of organizations. Organizations, hence, invest in security technologies and backup resources to try to minimize the damage caused from electronic criminal activities. In this dissertation, we seek to address how the organizations should decide on the level of their security infrastructure and specific technologies they use to address vulnerabilities in their information systems. In the first essay, we develop a market-based economic model in which the firm seeks to maximize the gains from information technology by investing in technology resources and attempt to limit the damage to resources through investment in security and backup infrastructure. The criminal strives to maximize the gains from successful exploitation of the vulnerabilities of the firm's resources. We evaluate the firm's and the criminal's decisions in response to variations in environmental parameters such as the punishment to criminals, the criminal skill level, the cost of resources, and the gains to the criminal. In the second essay, we develop an agent-based economy populated by the firm and the criminal agents that interact in an artificial environment. The agent-based approach provides us a platform to evaluate the theoretical predictions from the first essay through dynamic interaction between the agents in the economy. The third essay presents a Genetic Algorithm based approach to allow the organizations to select the security technology profile while minimizing the cost and maximizing the coverage of the vulnerabilities in information technology infrastructure.

1 COMPUTER CRIME AND SECURITY: AN ECONOMIC ANALYSIS

1.1 Introduction

In the twenty-first century, networked environments in the form of public Internet and private Intranets are ubiquitous. Email has become a primary channel of communication while the World Wide Web is changing how people collect and disseminate information. The ubiquity, openness, immediacy, and global reach of the Internet have brought about new opportunities for businesses. This interconnectivity has provided a medium for organizations to better manage their business activities while expanding to new markets and services.

Leveraging the benefits of global interconnectivity didn't come about without a new set of threats and risks. Illegal activities have persisted throughout human history and researchers have constantly tried to understand criminal behavior and evaluate the psychological (Clarke 1977; Hollin 1989) as well as the economic aspects of criminal activity (Becker 1968; Ehrlich 1996). The Internet provides an anonymous and connected environment where criminals, such as hackers, crackers, terrorist and foreign governments, can perpetrate their criminal activities by stealing information, denying service or by holding information and information resources for ransom. These criminals perpetrate illegal activities against firms computing resources, causing financial losses and damage to the reputation of the organization. Organizations invest in security technologies in order to counter these illegal activities or to limit the impact of these illegal activities on the firm.

In this paper, we intend to provide an economic model of computer crime that is perpetrated through the interconnected systems. We will develop a market-based economic model where both firms and criminals are incentive driven. Firms' incentives are in line with their information technology resources and they invest in security and

disaster recovery resources to minimize the damages. The criminal incentives are aligned toward the damages that they manage to cause to the firms. The model provides economic strategies for firms and criminals to follow in order to maximize their incentives.

1.2 Threat of Computer Crime

The threat of computer crime has increased over last several years. According to 2002 CSI/FBI survey (Power 2002) more than 60% of the interviewed IT professionals from various organizations reported intrusive activities against their information systems and 49% of the respondents reported breaches from outside sources. The percentage of respondents reporting intrusive activities from external agents has increased steadily over the last few years. Information Security Breaches Survey by Price Waterhouse Coopers (2002) reported that more than 76% of British firms that have online presence reported some kind of breach. This number was up from 69% reported in the year 2000. The CSI/FBI survey (Power 2002) also pointed out that the Internet connection has been the major source of point of attack on firms' information systems. The above threats can also be broken down to specific types of criminal activities that are perpetrated against the firms. They have identified independent hackers and business competitors as the main external sources of these attacks. A 2001 Industry Survey (Briney 2001) reported viruses (89% respondents), bugs in web browsers (48 %) and denial of service (39%) were the major concerns for the surveyed respondents. The CSI/FBI survey (Power 2002) identified virus attacks, denial of service, system penetration and the loss of proprietary information as the main source of damages to the firm. A 2002 Global Information Security survey by KPMG indicated 64% of Asian industries, 62% of European organizations and 55% of American organizations are affected by viruses every year.

Although the threat of computer crime has increased and still causes substantial damages to firms, the awareness in information security among firms has also increased. Most organizations are now implementing information security technologies to counter these attacks and limit damages. A CSI/FBI security survey (Power 2002) identified

anti-virus software, firewalls, intrusion detection systems, access control and encryption as the main security technologies used by organizations. A 2001 industry survey (Briney 2001) indicated that more than 50 % of the organizations use firewalls, authentication mechanism, anti-virus products and network sniffers to try to guard its resources against perpetrators.

Despite the increase in awareness of security technologies in organizations, Internet crime continues to have huge financial impact on organizations. The financial impact is either a result of damages suffered by organizations attacked in some capacity or is a result of investments that organizations make in security technologies to guard against these attacks. According to a CSI/FBI survey (Power 2002), the respondents reported more $170 million in damages in 2002 as compared to around $150 million in 2001. A Global Information Technology Survey reports that viruses ($10 million) were the major source of damages followed by equipment damage ($4 million), system failure ($ 3 million) and loss of data ($ 1 million). The above numbers are even more revealing if one takes into account the fact that respondents are reluctant to fully disclose the financial information on damages while reporting security breaches. Furthermore, a 2002 Information Security Survey reported that on average 10% of the organizations' information technology budget is used for security technologies. The number is much higher for smaller organizations. The Information Security Magazine Industry survey (Briney 2002) and Global Information Technology survey both reported that the financial sector is the leader in investments in security technologies followed by consulting organizations and educational institutions. "Price of Information Security", a research study by Gartner (2001) suggested that a large enterprise should invest approximately $650,000 on a yearly basis in information security management to minimize the risk of intrusion into organization resources.

The above surveys indicate that the problem of computer crime is a significant concern for organizations and has a huge economic impact on them. An economic model of computer crime should help organizations design some economic policies toward investment in security, technology and disaster recovery resources to minimize the effects

of computer crime on business operations. In this paper we attempt to construct such an economic model.

1.3 Economic Models of Crime

Economists for years have argued that both crime and demand for protection from crime are both motivated by the simple principle of accumulation of wealth (incentives). Economists have applied modern economic analysis to characterize crime and the activities undertaken to prevent these crime. Becker (Becker 1968) in his pioneering work presented a market based model for crime and punishment. He modeled the damage caused to society by crime as a function of the activity level of criminals. The criminal had monetary and psychological incentives to commit crime. However, if caught, the criminal was subject to punishment from the government. Becker also presented the situation where private investment in physical security by victims helped deter crime. Ehrlich (Ehrlich 1996) developed a 'market model' that assumed that the offender, a potential victim, buyers of illegal goods and services, and law enforcement authorities all behaved in accordance with the rules of optimizing behavior. He created a supply of offenses and demand for protection against crimes and explained the diversity of crime across time and space.

Viren (Viren 2001) proposed a supply of labor model in which criminal activities could be considered both as work and leisure. The criminal divided his time between labor, leisure and criminal activity part of which the criminal considered to be leisure. A Criminal derived utility from legal and illegal activities and disutility from punishment if apprehended during illegal activity. Cressman et al (Cressman, Morrison et al. 1998) developed a two-player game between property owners and potential criminals given exogenous levels of public policing and criminal sanctions. They used an evolutionary approach to show that the crime rate is cyclical over time and the average crime rate over the cycle is invariant on the magnitude of criminal sanctions. Cox (Cox 1994) also developed a two player game between the police and the public, where the public had a choice to engage in illegal activity (speeding) or not. In this model, if the public is

engaging in legal activity it does not care about the enforcement by police. However, if public is engaging in illegal activity it derived specific benefits from the illegal activity but paid fine if caught. The model also assumed that the police knew the distribution of public likely to engage in illegal activity. Lacroix and Marceau (Lacroix and Marceau 1995) developed a model through pair-wise interaction between the criminal and the owner. The owner made the protection decision while the criminal observed whether the owner is protected and thus made a decision on stealing. The criminal could not observe the value of property but knew the distribution of the value. The authors derived scenarios in which a criminal would attack protected or unprotected owners. Farmer and Terrell (Farmer and Terrell 2001) discussed the tradeoffs in a society that consisted of two groups with different crime rates. They created an economy with two types of people: innocent law abiding citizens and criminals who committed one crime each period and had no hope to reform, in a two period model. If a criminal was convicted in the first period, he/she spent the second period in jail. Farmer and Terrell presented scenarios where an innocent citizen may get convicted based on the evidence.

Baik et al (Hwan Baik 2001) developed a two-period model in which there is the possibility of social learning between the first and the second period. Individuals could commit crime over two periods while the enforcement authority could use fines to discourage such activity. The authors showed that it is desirable to punish first-time offenders as severely as repeat offenders. Jost (Jost 2001) presented a two-period model to investigate the situation where an individual's propensity to engage in an illegal activity is also dependent on the behavior of other individuals. During each period, individuals simultaneously decided whether to commit crime or not. The legal entity was responsible for convicting and punishing the offenders but they had a limited enforcement budget and could not convict all offenders. The authors argued that such a situation results in higher incentives for individuals to behave illegally.

Furlong (Furlong 1987) developed a general equilibrium model of crime by explicitly modeling the interaction among the criminals, victims of crime, and law enforcement agencies. Fender (Fender 1999) developed a general equilibrium settings where individuals who differed in their earnings abilities chose between work and crime,

while taking the probability of conviction and punishment into account. The author argued that agents with different earnings had different incentives to participate in crime. Garoupa (Garoupa 2000) extended the optimal law enforcement literature to organized crime. The author modeled a criminal organization as a vertical structure where the principal extracts some rent from agents through extortion. The author modeled the mafia as a profit-maximizing regulator that can not be punished by the government. Individuals who chose to commit crime to extract benefits have to pay the local mafia.

Marjit et al (Marjit, Rajeev et al. 2000) presented an incomplete information model where incomplete information available to the law enforcement agent may help to prevent crime where an agent was likely to engage in bribery. Andreoni (Andreoni 1991) argued that probability of conviction and magnitude of fine are not independent choice variables as implemented by most of the crime literature. They demonstrate that if the judicial system is based on a "reasonable doubt test", then the probability of conviction falls as the expected penalty for the crime increases.

The definition of crime covered in the above literature included murder, robbery, assault, theft, tax evasion, bribery etc. However, the new category of crime, i.e. electronic crime conducted using the communication medium and primarily targeting the computing and information resources, has not been researched using the above approach. The unique methods of perpetrating electronic crimes and their impact on today's highly interconnected e-commerce environment have warranted an independent analysis of such crimes. The above discussions have also helped us identify that the interactions between technology, security and backup investments and the punishments for the criminals and the criminal skill level are important issues for the organizations.

This research intends to use a market-based approach to present an economic analysis of the Internet crimes and its impact on organizations. The research intends to answer these questions: How should a firm react if the skill level of the attacker increases? What should be the strategy if the punishment levied to the attackers increases? In general, what are the more successful strategies to deter these Internet crimes? The model includes two categories of agents: criminal and firm. The criminal

perpetrates the illegal activities using the electronic medium. The firm is the targets of these criminal activities.

Table 1.1: The notation

Decision Variables	
T	Technology infrastructure
S	Security infrastructure
B	Backup resources
A	Criminal activity level
Parameters	
t	Technology cost rate
s	Security cost rate
b	Backup resource cost rate
v	Technology value rate
θ	Criminal skill level
a	Criminal effort rate
γ	Criminal gain rate
f	Punishment rate
L	Law enforcement activity level

1.4 The Model

The model in this paper uses the market-based framework for analyzing the economics of crime that was proposed by Becker and Ehlrich (Becker 1968; Ehrlich 1996). The model assumes two categories of agents who try to optimize their decisions based on the assumptions for the behavior of the other agent. The two categories of agents used in the model are the firm and the criminal. Firm is an agent that represents organizations that invest in information technologies for the business productivity gains. Criminal is an agent representing criminal elements, such as hacker, terrorists and organized crime, who engage in illegal activities over the Internet. We are using a representative agent model where the firm is representative of all other firms and the criminal is representative of all criminals. The firm agent tries to optimize the decision to invest in technology, security and disaster recovery infrastructure. On the other hand, the

attacker tries to optimize the activity level to maximize gains from damages caused to the firms. This section presents the construct for the model and the decisions of the individual agent given the behavior of the agent of the other category. The notation used in the model is summarized in Table 1.1.

1.4.1 The Firm

The firm agent represents business organizations that use Information Technology to gain efficiency or to use technology as a strategic advantage. The firm invests in information technology infrastructure to support its business processes and generate value for the firm. Let the technology infrastructure level of the firm be given by T, then value V generated from the resources and the cost of the technology C_1 are given by (1.1) & (1.2). We assume the cost to be linear to compensate for the complexity of the technology as well as the economies of scale. The cost of technology increases at a growing rate as the additional technology adds to the complexity of the system. However, the firm can also leverage the advantages of economies of scale by increasing the investment in technology infrastructure.

$$V = vT \tag{1.1}$$

$$C_1 = tT \tag{1.2}$$

The firm is vulnerable to attacks from hackers, terrorists and/or competitors who try to break into the firm's information technology resources. The exploitation of these vulnerabilities present in information technology results in damages to the firm. These damages can be direct damages through loss of resources, loss of customer trust, loss of proprietary information, loss of business due to system outage or losses from damaged reputation. The firm invests in security technologies to reduce the probability of attacks being successful. Security technologies such as firewalls, Intrusion Detection Systems and encryption systems work towards reducing the chance that any unauthorized party can gain access to resources and cause damage to them. Let the security infrastructure for the firm be denoted by S, then the security level of the firm is given by (1.3). The cost of security infrastructure is given by (1.4) (2001). The probability of a successful

attack against the firm's resources is given by (1.5), where θ represents the skill level of the criminal and A represents the activity level of the criminal.

$$\psi = \frac{S}{T} \tag{1.3}$$

$$C_2 = sS \tag{1.4}$$

$$\rho = \frac{\theta A}{S} \tag{1.5}$$

The security technology not only helps in preventing the successful attacks against the firm's information technology resources but also helps in limiting the losses to the firm from damages caused to the resources or stolen information. Security technologies such as, the Intrusion Detection System, help identify a malicious activity taking place on the firm's information networks and limit the spread of damage to additional resources. Anti-virus software prevents the spread of the virus through the firm's computing system and limits damage to systems through quarantine of infected resources. Apart from security technologies, the firm can also limit the damage caused to the information technology infrastructure by planning for disaster recovery and investing in disaster recovery of the systems. One common technique for limiting the damage is through an investment in backup resources. The firm can create back up copies of data in case the data gets corrupted to prevent any loss of information. The firm can also invest in backup information technology infrastructure to prevent interruption of service in the event of an attack damaging some computing resources. Let the investment in backup resources by the firm be B, then the cost of backup resources is given by(1.6). The damage limitation factor g represents the factor by which the damage to the firm is limited and is given by (1.7).

$$C_3 = bB \tag{1.6}$$

$$g = T(1 - B) \tag{1.7}$$

The actual damage caused to the firm in case an attack is successful is now given by ,

$$D = \theta A \frac{g}{\psi} \tag{1.8}$$

We assume a normalized model by normalizing the values of T, S and B to $[0,1]$, i.e. $T,S,B \in [0,1]$. We also assume T, S and B to be continuous variables. The information system's budget for the firm is limited and the budget has to be divided among information technology, backup and security infrastructure. If we assume the normalized budget of a firm to be 1 then the budget constraint is given by (1.9),

$$tT + sS + bB \leq 1 \tag{1.9}$$

The objective of the firm is to maximize the value to the firm minus the damages caused to the resources while satisfying the budget constraint. The objective function of the firm is given by (1.10)

$$\begin{aligned} &\underset{B,S,T}{Max}\, \Pi = V - D\rho \\ &subject\ to \\ &tT + sS + bB \leq 1 \end{aligned} \tag{1.10}$$

1.4.1.1 First Order Conditions for the Firm

Since, we are solving a maximization problem with a budget constraint we can represent the budget constraint as binding, therefore the optimization problem for the firm is now,

$$\begin{aligned} &\underset{B,S,T}{Max}\, \Pi = V - \frac{\theta^2 A^2 (1-B) T^2}{S^2} \\ &subject\ to \\ &tT + sS + bB = 1 \end{aligned} \tag{1.11}$$

Eliminating one variable from the budget constraint into the optimization function we can get first order conditions with respect to S and T given by (1.12) & (1.13)

$$\Pi_T = v - \frac{\theta^2 A^2 \left[2(b-1)T + 2sST + 3tT^2 \right]}{bS^2} = 0 \tag{1.12}$$

$$\Pi_S = \frac{\theta^2 A^2 T^2 \left[2(b-1) + sS + 2tT \right]}{bS^3} = 0 \tag{1.13}$$

From the above we can find the strategies that the firm can employ if it knows the skill level and the activity level of the criminal. Although these strategies are not socially

optimal strategies, they do give some idea about how the firm would respond if it were attacked. If the firm knew the mix of attacker skill level and the activity level the strategies of the firm would be given by (1.14), (1.15) & (1.16).

$$T = \frac{(1-b)}{t}\left[1 - \frac{\theta A s}{\sqrt{\theta^2 A^2 s^2 + 4vbt}}\right] \tag{1.14}$$

$$S = 2\frac{(1-b)\theta A}{\sqrt{\theta^2 A^2 s^2 + 4vbt}} \tag{1.15}$$

$$B = 1 - \frac{(1-b)\theta A}{b\sqrt{\theta^2 A^2 s^2 + 4vbt}} \tag{1.16}$$

1.4.2 The Criminal

The criminal agent represents the perpetrators such as, hackers, terrorists, business competitors, foreign governments, organized crime or any other entity involved in computer crime against the information systems of any organization. The criminal derives psychological, political or financial benefits from perpetrating attacks (Briney 2002). A hacker derives psychological gains by proving that he/she is capable of exploiting the vulnerabilities in the firm's information systems. A business competitor derives financial gains by stealing proprietary information that gives it a competitive advantage. A terrorist can exploit the vulnerabilities to hold the firm hostage to meet its political motives. Irrespective of how these agents derive their benefits, they indulge in criminal activities to cause damage to the firm's information system. We assume that the criminal maintains an activity level A to exploit the vulnerability of information systems. The criminal has a skill level, $\theta \in [0,1]$ where 1 represents maximum skills and 0 represents no skills. We assume θ and A to be continuous variables. The gain that the criminal derives from perpetrating an attack against a firm's resources is given by (1.17) where γ is the gain parameter. The gain parameter is modeled as a representative of the gain of specific types of criminal. Each criminal derives different gain from causing the same amount of damage to a firm. We model the gain as a parameter and later perform

comparative statics with respect to gain to analyze the gains of different types of criminals.

$$G = \gamma \rho D \tag{1.17}$$

Or,

$$G = \gamma \theta^2 A^2 \frac{(1-B)T^2}{S^2} \tag{1.18}$$

However, the criminal has to exert effort to maintain the activity level. The effort exerted by the criminal represents the costs to the criminal to perpetrate criminal activities. These costs could be the actual resources that the criminal consumes to perpetrate attacks or the cost of opportunity if the criminal had spent that effort in some other legal activity. The effort exerted by the criminal is given by (1.19),

$$E = aA^2 \tag{1.19}$$

The effort cost is not the only cost that the criminal faces. There is a chance that the criminal can be caught by law enforcement agencies and get punished. The criminal, if caught and convicted, pays fine proportional to the damage caused to the firm. The probability of catching the criminal depends on the activity level that the law enforcement agency maintains and the security infrastructure of the firm. The security technologies can help identify the intruder leading to the capture of the criminal. If the law enforcement activity level is given by L, then the probability that the attacker is caught is given by (1.20)

$$\lambda = (1-\theta) A \psi L \tag{1.20}$$

The punishment that the criminal faces, if caught and convicted, is modeled as a fine (Becker 1968). The jail term can also be modeled as a fine because of the loss of opportunity for the criminal to earn income through legal or illegal means. If the fine rate is f, the fine that the criminal faces is given by

$$F = f \rho D \tag{1.21}$$

Or,

$$F = f \theta^2 A^2 \frac{(1-B)T^2}{S^2} \tag{1.22}$$

Now the objective of the criminal is to maximize the gains from the illegal activities while minimizing the effort and the punishment by the law enforcement agencies. The objective function of the criminal is given by (1.23) &(1.24),

$$\underset{A}{Max}\,\Gamma = G - E - \lambda F \tag{1.23}$$

Or,

$$\underset{A}{Max}\,\Gamma = \frac{\gamma\theta^2(1-B)T^2}{S^2}A^2 - aA^2 - \frac{(1-\theta)\theta^2 fL(1-B)T}{S}A^3 \tag{1.24}$$

1.4.2.1 First Order Conditions for the Criminal

The first order condition for the criminal is given by,

$$\Gamma_3 = 2\left[\gamma\theta^2\frac{(1-B)T^2}{S^2} - a\right]A - 3(1-\theta)\theta^2 fL\frac{(1-B)T}{S}A^2 \tag{1.25}$$

From the above, we can find the strategy that the criminal should employ if the technology, security and the disaster recovery levels of the firm were known, i.e. if the criminal knew the technology mix that the organization possesses. The strategy of the criminal is given as

$$A = \frac{2}{3}\frac{1}{(1-\theta)fL}\left[\gamma\frac{T}{S} - a\frac{S}{\theta^2(1-B)T}\right] \tag{1.26}$$

1.5 The Results

The primary objective of the model is to identify the strategies that the firm and the criminal should pursue for different environmental conditions. We are more interested in finding out how the firm should change the investments in information technology, security and back up infrastructure if the prices of resources change, the skill profile of the criminal changes or the punishment levied on the criminal changes. Similarly, from the criminal's perspective we seek to identify how the attacker should change the activity level in response to changes in parameters. Comparative statics can be performed on all variables to analyze the effects of variations in the parameters on the

decisions of the agents. For performing comparative statics, we take total differentials of first order conditions. The equations used for comparative statics are given by (1.27) where H is any parameter with respect to which we are performing comparative statics.

$$\begin{aligned}
&-\left[\frac{v}{T}+3\frac{\theta^2A^2tT}{bS^2}\right]dT+2\frac{\theta^2A^2tT^2}{bS^3}dS-2\frac{v}{A}dA=-\Pi_{HT}dH\\
&2\frac{\theta^2A^2tT^2}{bS^3}dT+\frac{\theta^2A^2sT^2}{bS^3}dS=-\Pi_{HS}dH\\
&\left[2\frac{aA}{T}+\frac{\gamma\theta^2AsT}{bS^2}\right]dT-\left[2\frac{aA}{S}+\frac{\gamma\theta^2AsT}{bS^3}\right]dS+\left[2a-\frac{\gamma\theta^2sT^2}{bS^2}\right]dA=-\Gamma_{HA}dH
\end{aligned} \tag{1.27}$$

1.5.1 Comparative Statics with respect to the Punishment Level:

Totally differentiating the first order condition or substituting f for H in equation (1.27), we see that the variations in decision variables as the punishment level or the fine rate for the criminals is varied. Performing the comparative statics on the punishment level, we obtain the following for the Security level for the firm.

$$\frac{dS}{df}=6\frac{(1-\theta)\theta^2ALstvS^2T^2}{\left[\left(2a-\frac{\gamma\theta^2sT^2}{bS^2}\right)\left[\left(3sS+4tT\right)\theta^2A^2T^2t+bsvS^3\right]-2v\left(2abS^2+\gamma\theta^2T^2s\right)\left(sS+2tT\right)\right]} \tag{1.28}$$

From first order conditions,

$$2a-\frac{\gamma\theta^2sT^2}{bS^2}<0 \tag{1.29}$$

From above we arrive at the following proposition

Proposition 1: *As the punishment to the criminal for perpetrating crime against the firm's resources increases, the Security infrastructure of the firm decreases*.

Remark: The above proposition implies that if the law governing the crimes against information systems changes and the criminal is dealt much harsher punishment, then the firm can assume that the criminal is going to get discouraged and reduce the activity level. Hence, the firm can choose to reduce the security infrastructure.

Performing comparative statics on the punishment level for technology level we obtain:

$$\frac{dT}{df} = -3\frac{(1-\theta)\theta^2 ALs^2 \quad vS^2T^2}{\left[\left(2a - \frac{\gamma\theta^2 sT^2}{bS^2}\right)\left[\left(3sS + 4tT\right)\theta^2 A^2T^2t + bsvS^3\right] - 2v\left(2abS^2 + \gamma\theta^2T^2s\right)\left(sS + 2tT\right)\right]} \tag{1.30}$$

From the above we arrive at the following proposition

Proposition 2: *As the punishment to the criminal for causing damage to a firm's resources increases, the Information Technology infrastructure of the firm increases*.

Remark: The above proposition implies that if the punishment to the criminal increases, they would be less motivated to carry out attacks, enabling the firm to invest more in information technology infrastructure without fearing attacks from the criminal.

Performing comparative statics on the punishment level for backup resources we obtain:

$$\frac{dB}{df} = -3\frac{(1-\theta)\theta^2 ALs^2 tvS^2T^2}{b\left[\left(2a - \frac{\gamma\theta^2 sT^2}{bS^2}\right)\left[\left(3sS + 4tT\right)\theta^2 A^2T^2t + bsvS^3\right] - 2v\left(2abS^2 + \gamma\theta^2T^2s\right)\left(sS + 2tT\right)\right]} \tag{1.31}$$

Proposition 3: *As the punishment to the criminal increases, the backup infrastructure of the firm increases*.

Remark: The above proposition indicates that if the punishment to the criminal increases, it is prudent for the firm to increase the technology infrastructure. The firm expects the criminal to have less incentive to indulge in criminal activity. Hence, the firm prefers to limit the damage caused by investing in backup resources, instead of trying to provide more security to the systems.

Performing comparative statics on punishment level for criminal activity level we obtain,

$$\frac{dA}{df}=\frac{3(1-\theta)\theta^2A^2LsT}{2b\left[\left(2a-\frac{\gamma\theta^2sT^2}{bS^2}\right)-2\frac{v\left(2abS^2+\gamma\theta^2T^2s\right)\left(sS+2tT\right)}{\left[\left(3sS+4tT\right)\theta^2A^2T^2t+bsvS^3\right]}\right]S} \tag{1.32}$$

Proposition 4: *As the punishment to the criminal increases, the criminal activity level decreases.*

Remark: The above proposition provides a very intuitive result. It says that it is prudent for the criminal to reduce the activity level when facing severe punishment.

1.5.2 Comparative Statics with respect to Criminal Skill Level

Totally differentiating the first order condition with respect to the decision variable and the criminal skill level, we can arrive at the comparative static results with respect to the criminal's skill level. We obtained the following results when we performed the comparative statics,

$$\frac{dS}{d\theta}=-\frac{\frac{2ab(2-3\theta)S^2+\gamma\theta^3T^2s}{1-\theta}+\left(\gamma\theta^2T^2s-2abS^2\right)}{b\left[\left(2abS^2-\gamma\theta^2sT^2\right)\left[\frac{s}{4bS^2Tt}+\frac{3\theta^2A^2Ts}{4b^2S^4v}+\frac{\theta^2A^2T^2t}{b^2S^5v}\right]-\frac{\left(2abS^2+\gamma\theta^2T^2s\right)\left(sS+2tT\right)}{2bS^3Tt}\right]\theta S^2} \tag{1.33}$$

From first order conditions

$$2abS^2-\gamma\theta^2sT^2<0 \tag{1.34}$$

From above we get,

$$\begin{aligned}\frac{dS}{d\theta}>0 \text{ if } \theta\le\frac{2}{3}\\ \frac{dS}{d\theta}<0 \text{ if } \theta>\frac{2}{3}\end{aligned} \tag{1.35}$$

The above leads us to the following proposition

Proposition 5: *As the skill level of the criminal increases, the security infrastructure of the firm increases to a threshold skill and then it decreases.*

Remark: As the skill level of the criminal increases, it is prudent for the firm to keep increasing security. However, above a certain skill level it is no longer beneficial for the firm to invest in security infrastructure, since additional security does not result in reduction in the threat level. In such a scenario, it is better to decrease the security to limit the cost of security and rely on disaster recovery.

Analyzing the effects of skill level on the backup resources of the firm we get,

$$\frac{dB}{d\theta}=\frac{s\left[\frac{2ab(2-3\theta)S^2+\gamma\theta^3T^2s}{1-\theta}+\left(\gamma\theta^2T^2s-2abS^2\right)\right]}{2b^2\left[\left(2abS^2-\gamma\theta^2sT^2\right)\left[\frac{s}{4bS^2Tt}+\frac{3\theta^2A^2Ts}{4b^2S^4v}+\frac{\theta^2A^2T^2t}{b^2S^5v}\right]-\frac{\left(2abS^2+\gamma\theta^2T^2s\right)\left(sS+2tT\right)}{2bS^3Tt}\right]\theta S^2} \tag{1.36}$$

Proposition 6: *As the skill level of the criminal increases, the backup resources of the firm decrease up to a point and then they increase*.

Remark: As the skill level of the criminal increases, below a certain threshold skill level, the firm should focus more on security infrastructure and increase the security but reduce backup resources. However, above the threshold skill level, it is more prudent for the firm to increase backup resources and try to limit the impact of attack rather than increase security in an attempt to limit the probability of a successful attack.

Analyzing the effects of the skill level on the activity level of the criminal we get,

$$\frac{dA}{d\theta}=-\frac{A}{\theta}\left[1+\frac{2STt\left(\frac{2ab(2-3\theta)S^2+\gamma\theta^3T^2s}{1-\theta}+\left(\gamma\theta^2T^2s-2abS^2\right)\right)}{\left[\left(2abS^2-\gamma\theta^2sT^2\right)-\left(2abS^2+\gamma\theta^2T^2s\right)\left(sS+2tT\right)\left(\frac{s}{4tT}+\frac{3\theta^2A^2Ts}{4bS^2v}+\frac{\theta^2A^2T^2t}{bS^3v}\right)\right]}\right] \tag{1.37}$$

Proposition 7: *As the skill level of the criminal increases, the activity level of the criminal decreases beyond a certain threshold skill.*

Remark: As the skill level of the criminal increases, the criminal should increase the activity level to a certain threshold but beyond that threshold it is better for the criminal to start decreasing the activity level with increase in skill. This may be because

after that point the criminal faces much stricter penalties if caught. However, with increased skills the criminal still has a good chance to successfully cause more damage to the firm.

1.5.3 Comparative Statics with respect to the Criminal Effort Cost

Totally differentiating the first order condition with respect to the decision variable and the criminal effort cost, we can arrive at the comparative static results with respect to the criminal effort cost. We obtained the following results when we performed the comparative statics,

$$\frac{dA}{da} = 2\frac{A}{\left(2a - \frac{\gamma\theta^2 sT^2}{bS^2}\right) - 2\frac{v\left(2abS^2 + \gamma\theta^2T^2s\right)\left(sS + 2tT\right)}{\left[\left(3sS + 4tT\right)\theta^2A^2T^2t + bsvS^3\right]}} \tag{1.38}$$

Proposition 8: *As the criminal effort cost increases, the criminal activity level decreases*.

Remark: The above proposition presents a very intuitive result. As the cost of illegal activities to the criminal increases, the criminal should reduce the activity level.

Analyzing the effects of the criminal effort costs on the security level of the firm we get,

$$\frac{dS}{da} = 8\frac{vt}{\left(2a - \frac{\gamma\theta^2 sT^2}{bS^2}\right)\left(\left(3sS + 4tT\right)\theta^2A^2T^2t + bsvS^3\right) - 2\frac{v\left(2abS^2 + \gamma\theta^2T^2s\right)\left(sS + 2tT\right)}{bS^3Ts}} \tag{1.39}$$

Proposition 9: *As the costs to the criminal increase, the security infrastructure of the firm decreases*.

Remark: The above proposition states that as the costs to the criminal, for indulging in illegal activity against the firm's resources, increase, the firm security

infrastructure should decrease. The attacker reduces the activity level when costs rise, thereby, enabling the firm to reduce the security infrastructure.

1.5.4 Comparative Statics with respect to Security Cost

Totally differentiating the first order conditions with respect to the decision variables and the security cost, we arrive at the following comparative statics results:

$$\frac{dS}{ds} = -\frac{\left[\left(2abS^2 - \gamma\theta^2 sT^2\right)\left(\theta^2 A^2 T^2 t - bS^2\right) + \left(4ab^2 S^4 + 2b\gamma\theta^2 S^2 T^2 sv\right)\right] S^2}{\left(\gamma\theta^2 T^2 s - 2abS^2\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] + 2\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)bS^2 v} \tag{1.40}$$

Proposition 10: *As the security cost increases, the security infrastructure of the firm decreases*.

Remark: This is an intuitive result, indicating that the firm should reduce the security infrastructure if the cost of security increases.

1.5.5 Comparative Statics with respect to Technology Cost

Totally differentiating the first order conditions with respect to decision variables and the technology cost, we arrive at the following comparative statics results:

$$\frac{dS}{dt} = -\frac{\left(2abS^2 + 3\gamma\theta^2 T^2 s\right)bS^3 Tv}{-\left(\gamma\theta^2 T^2 s - 2abS^2\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] + 2\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)bS^2 v} \tag{1.41}$$

Proposition 11: *As the technology cost increase, the security infrastructure of the firm decreases*.

Remark: The above proposition indicates that if the cost of the technology increases, the firm should invest less in security infrastructure. This could be explained from the fact that if the cost of technology increases, the firm will most probably decrease the technology infrastructure, thereby allowing the firm to reduce security.

Analyzing the effects of technology cost on the criminal activity level:

$$\frac{dA}{dt} = -\frac{\left(2abS^2 + 3\gamma\theta^2T^2s\right)\left(sS + 2tT\right)\theta^2A^3T^2}{\left(2abS^2 - \gamma\theta^2T^2s\right)\left[\left(3sS + 4tT\right)\theta^2A^2T^2t + bsvS^3\right] - 2\left(2abS^2 + \gamma\theta^2T^2s\right)\left(sS + 2tT\right)bS^2v} \tag{1.42}$$

Proposition 12: *As the technology cost increase, the activity level of the criminal decreases*.

Remark: If the technologies cost increases, the firm is most probably going to reduce the technology infrastructure. If the technology infrastructure is reduced, the criminal will have less incentive to increase the activity level, as they might not get any additional benefit because of it.

1.5.6 Comparative Statics with respect to Technology Value

Totally differentiating the first order conditions with respect to technology value and the decisions variables we obtain:

$$\frac{dA}{dv} = -\frac{\left(2abS^2 + 3\gamma\theta^2T^2s\right)\left(sS + 2tT\right)bAS^2}{\left(2abS^2 - \gamma\theta^2T^2s\right)\left[\left(3sS + 4tT\right)\theta^2A^2T^2t + bsvS^3\right] - 2\left(2abS^2 + \gamma\theta^2T^2s\right)\left(sS + 2tT\right)bS^2v} \tag{1.43}$$

Proposition 13: *As the value of the technology increases, the activity level of the attacker increases*.

Remark: If the value of technology increases, the firm is going to invest more in technology, giving more incentive for the criminal to increase the activity level.

$$\frac{dT}{dv} = \frac{\left(2abS^2 - \gamma\theta^2sT^2\right)bsTS^3}{\left(2abS^2 - \gamma\theta^2T^2s\right)\left[\left(3sS + 4tT\right)\theta^2A^2T^2t + bsvS^3\right] - 2\left(2abS^2 + \gamma\theta^2T^2s\right)\left(sS + 2tT\right)bS^2v} \tag{1.44}$$

Proposition 14: *As the value of the technology increases, the technology infrastructure of the firm increases*.

Remark: If the value of technology increases, the firm invests more in technology to leverage the additional benefit from the technology.

Analyzing the effects of the technology value on the security level of the firm

$$\frac{dS}{dv} = -2\frac{\left(2abS^2 - \gamma\theta^2 sT^2\right)b^2 S^5 Ttv}{\left(2abS^2 - \gamma\theta^2 T^2 s\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] - 2\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)bS^2 v} \tag{1.45}$$

Proposition 15: *As the value of the technology increases, the security infrastructure of the firm decreases*.

Remark: If the value of technology increases, the firm invests more in technology to increase benefit from technology; furthermore it is more beneficial for the firm to limit the damages rather than to prevent the attacks altogether.

$$\frac{dS}{dv} = \frac{\left(2abS^2 - \gamma\theta^2 sT^2\right)sbS^5 Ttv}{\left(2abS^2 - \gamma\theta^2 T^2 s\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] - 2\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)bS^2 v} \tag{1.46}$$

Proposition 16: *As the value of the technology increases, the backup infrastructure of the firm increases*.

Remark: If the value of the technology increases, it is more prudent for the firm to limit the damage from attacks instead of trying to invest in security to prevent these attacks.

1.5.7 Comparative Statics with respect to Criminal Gain

Totally differentiating the first order conditions with respect to the decision variable and the criminal gain we obtain:

$$\frac{dS}{d\gamma} = -4\frac{b\theta^2 S^3 T^3 stv}{\left(2abS^2 - \gamma\theta^2 T^2 s\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] - 2\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)bS^2 v} \tag{1.47}$$

Proposition 17: *As the criminal gain increases, the security of the firm increases*.

Remark: If the criminal gain increases, the criminal is likely to increase the activity level. This necessitates that the firm increase the security infrastructure to counter the increase in activity of the criminal.

Analyzing the effects of the criminal gain on the technology we get,

$$\frac{dT}{d\gamma} = 2\frac{b\theta^2 S^3 T^3 s^2 v}{\left(2abS^2 - \gamma\theta^2 T^2 s\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] - 2\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)bS^2 v} \tag{1.48}$$

Proposition 18: *As the criminal gain increases, the technology infrastructure of the firm decreases*.

Remark: If the criminal gain increases, the criminal is likely to increase the activity level too. This necessitates the firm to decrease the technology level to limit the damage.

Analyzing the effects of the criminal gain on the criminal activity level,

$$\frac{dA}{d\gamma} = -\frac{\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right]\theta^2 AT^2 s}{\left(2abS^2 - \gamma\theta^2 T^2 s\right)\left[\left(3sS + 4tT\right)\theta^2 A^2 T^2 t + bsvS^3\right] - 2\left(2abS^2 + \gamma\theta^2 T^2 s\right)\left(sS + 2tT\right)bS^2 v} \tag{1.49}$$

Proposition 19: *As the criminal gain increases, the activity level of the criminal increases*.

Remark: If the criminal gain increases, the criminal has more incentive to increase the activity level to cause more damages to the firm and get more gains as a result.

Table 1.2: Comparative Statics Results

Variable Parameter	Technology T	Security S	Back up B	Criminal Activity A
f	↑	↓	↑	↓
θ	↓↑	↑↓	↓↑	–↓
a	↑	↓	↑	↓
γ	↓	↑	↓	↑
v	↑	↓	↑	↑
s	–	↓	–	–
b	–	↓	–	–
t	–	↓	↑	↓

1.6 Conclusions

In this paper we have created an economic model of crime that tries to model the behavior of incentive driven firms and criminals. We have tried to evolve strategies for both the firm and the criminal when environmental conditions change. All the results of comparative statics are summarized in Table 1.2. The results indicate that as the conviction and punishment of the criminal increases, the criminal has less incentive to indulge in illegal activities. This finding is consistent with the standard literature on economics of crime that claims that punishment acts as a deterrent to the criminals. The result also indicates when the punishment increases; the firm can afford to reduce private security (information security) for computer systems. However, in such a scenario the model suggests that it is much more beneficial for the firm to address illegal activities by investing more in disaster recovery measures and limiting the impact of successful illegal activities against the firms.

The other results seem to indicate that if the skill level for the criminal increases, the firm should increase the information security infrastructure to counter the increased skill of the criminal. However, after a certain skill level it is no longer beneficial for the firm to increase the investment in information security. The model suggests that the firm no longer has any additional incentive to increase security. However, the firm attempts to limit the damages caused from a successful attack by investing more in disaster recovery.

It is also interesting to note that the criminal should actually reduce the activity level if it is highly skilled and the skill level increases further.

From the above model we can conclude that it is not always an optimal strategy for the firm to invest in information security to counter the intrusive or illegal activities of the criminals against the firm's information systems. It can also be concluded that the firm should strive for a mixture of security technologies and disaster recovery measures to neutralize the illegal activities.

This research is a representative agent model and does not take into account the presence of different types of firms or criminals in the environment. A future extension of this research may include a probability distribution of criminals and simultaneously modeling a class of criminals. We only considered the external criminal and did not model the malicious or non-malicious internal sources of security breaches. It would be interesting to study the impact of insider breaches on the security strategies of the organization.

2 AGENT-BASED APPROACH FOR ANALYZING THE INFORMATION SECURITY STRATEGIES FOR AN ORGANIZATION

2.1 Introduction

Over the past few years, the Internet and information systems have become an integral part of organizations looking to exploit the interconnectivity of the Internet and efficiency of information technology for business advantages. However, the Internet has also given rise to a new set of illegal activities that can be perpetrated through the interconnected systems. These activities can constitute a virus attack, denial of service to authorized users of the resources, theft of information, fabrication of data or even physical damage to the resources. According to a recent CSI/FBI survey (Power 2002) more than 60 % of interviewed organizations reported such illegal activities against their computing resources. The CSI/FBI survey reported more than $170 million damages to organizations, as a result of these illegal activities, in 2002, an increase of about 12% over the year before. As a result, organizations are looking to invest in information security technologies, such as firewalls, some form of authentication mechanism, anti-virus software, and intrusion detection systems, to protect the computing resources from the illegal activities. A 2001 Industry survey (Briney 2001) indicates that more than 50% of the surveyed firms used these technologies to counter the illegal activities that are perpetrated to computing resources through the online medium.

This increase in computing crime has resulted in researchers attempting to address this problem from an economic point of view. Becker, Ehlrich (Becker 1968; Ehrlich 1996) and other economists have developed rational models of crime where they assume that the organizations as well as the criminals are acting in a rational manner and are trying to optimize their own incentives. The first essay created an economic model of computer crime where the organization's focus was to optimize benefit from information

technology while minimizing the success of and damage from the illegal activities perpetrated against its information systems. Criminals optimized their criminal activity to maximize gains while trying to minimize the chance of getting caught. However, these economic models fail to capture the dynamic nature of interactions taking place amongst these agents.

In this paper, we attempt to construct an agent-based economy for computer crime. Over the past few years the interest among agent-based computation economics has increased since it provides a bottom up approach to construction of an economic environment with room for the evolution of strategies. Our economy will consist of firms and attackers that interact in an artificial environment. An agent based model would better capture the dynamic nature of interactions between firms and attackers.

2.2 Agent-Based Economies

A significant amount of research has been done in the field of agent-based economies. Economists defined agent-based economies to be one where economic agents interact in a distributed environment resulting in complicated dynamic systems giving rise to macro economic regularities (Tesfatsion 2002). Significant progress has been made in the research of agent based economies and researchers have implemented economies to model the interactions between agents or have created evolving agents that adapt their behavior to environmental conditions. Researchers have also implemented human-computer agent experiments or have provided tools for creation of completely agent-based economies.

Smith (Smith 1994) argued that laboratory experiments can not only be used for validating and exploring the current theories but also for comparing different environments and institutions. He argued that by using identical environments and varying the rules of exchange, comparative properties of institutions could be established. Similarly, by varying the environments, the robustness of the institution can be established. Roth (Roth 1988) studied different sets of laboratory experiments and suggested that laboratory experiments in economic environments could help create

controlled settings and provide agents access to draw inferences about the economic setting as well as the impact of the environment.

Arthur (Arthur 1991) explored the construction of theoretical economic agents that behave like actual human agents and used them in artificially created computational economies. He demonstrated that the artificial agents could replicate human behavior in limited settings while simultaneously learning over time too. Batten (Batten 2000) examined the behavior of adaptive economic agents as they gained knowledge. Batten also described how these agents co-evolve and learn by interacting. He demonstrated that some agents showed the quality of being innovative explorers while others were just content to be imitators. Using the agent-based computational experiments, Axelrod (Axelrod 1986) demonstrated how self-interested non-related agents cooperated through reciprocity. Epstein (Epstein 2001) presented an agent-based model that captured a particular phenomenon: that individual thought is often inversely related in strength to social norm. Vriend (Vriend 2000) demonstrated that there was a difference between individual and social learning and illustrated the consequences of choosing a specific computational tool using two variants of Genetic Algorithms.

Rust (Rust, Miller et al. 1994) presented comparative analysis of thirty trading programs that participated in a double auction tournament. Rust found that a simple rule-of-thumb is an effective and robust performer over a wide range of trading environments. Gode and Sunder (Gode and Sunder 1993) presented market experiments in which human traders are replaced by "zero-intelligence" programs that submitted random bids and offers. Using these agents they demonstrated that the allocative efficiency of the double auction derives from its structure and is independent of trader's motivations and intelligence. Marks (Marks 1992) used computer strategies to demonstrate that oligopolistic pricing competitors could successfully compete. In another study, Marks used (Marks 1998) data from the retail coffee market in an artificial economy to evolve optimal oligopolistic partitioning and showed that brand managers used very little information irrespective of price changes. Klos (Klos and Nooteboom 2001) used an agent-based economy to model development of transactions between firms. In their model the agents adapt trust in a partner as a function of loyalty. Arthur et al (Arthur

1997) created a dynamic theory of asset pricing based on agent based heterogeneous traders who update their price preferences individually using classifier systems.

In this paper, we use a similar agent-based economy to model interactions between profit seeking firms that invest in information technology for its operational, strategic and competitive benefits, and the criminals that seek psychological, political and financial gains by indulging in illegal activities against the information technology resources of the firm. The firms as well as the criminals use a combination of strategies to optimize their goals. We will evaluate the impact of various strategies in the artificial economy under different environmental conditions.

2.3 Agent Design and Specifications

We use an agent-based model with two categories of agents – the firms and the criminals. The firms represent organizations that invest in information technology to gain the advantages of efficiency and connectivity of technology. However, they also invest in security and backup resources to prevent and deter any illegal activity against their resources. Criminals perpetrate illegal activities against firms' computing resources to gain psychological, political, social and financial gain. In the model, each of these agents has to make decisions about their decision variables at the beginning of each period. Contingent on the decisions made by the agents, each agent possesses certain behaviors or properties that define the characteristics of the agent for that period. The two types of agents interact in an open environment during each period, i.e. the criminals try to attack the resources of firms. The extent of success or failure of these attacks is dependent on the characteristics of individual interacting agents. In this paper, we use the agent definitions that are analogous to the one defined in the first essay. The agent specifications are described below:

2.3.1 Firms

Firms have three decision variables:

Variable 1: Technology, $T \in [0,1]$ and is continuous and independent

Firms invest in information technology to exploit the efficiency of the technology and to gain competitive advantage. At the beginning of each period, firms have to decide on what should be their technology infrastructure should be.

Variable 2: Security, $S \in [0,1]$ and is continuous and independent

Firms are targets of attacks against its information resources. Firms can invest in security technologies that help reduce the probability of such attacks and limit the damages from successful attacks. At the beginning of each period, firms make decisions on their security infrastructure.

Variable 3: Backup Resources, $B \in [0,1]$ and is continuous and independent

If the attacks against the firms' information systems are successful, firms need to be prepared to recover as soon as possible from the damages suffered. Firms invest in backup resources to try to limit the damages from attacks. At the beginning of each period, firms decide on their back up resources.

Once firms have made their decisions for the period, the properties and behaviors of each firm are computed. The first set of properties is the costs of these decisions to the firm, i.e. the cost of technology infrastructure, security infrastructure and the back up resources. These costs are:

Technology infrastructure cost

$$C_1 = tT \tag{2.1}$$

Security infrastructure cost

$$C_2 = sS \tag{2.2}$$

Backup infrastructure cost

$$C_3 = bB \tag{2.3}$$

Firms also have the benefits from the investment in technology that is given by,

$$V = vT \tag{2.4}$$

where, $v,t,s,b \in [0,1]$ are the value and cost parameters for technology, security and backup resources and are set externally in the agent-based economy. These parameters are continuous and independent.

Firms invest in security technologies to reduce the probability of success of the attacks as well as to limit the damage caused to the firm. Each firm's security level is defined as

Security Level

$$\psi = k_{\psi} \frac{1}{T(1-S)} \tag{2.5}$$

where, k_{ψ} is the security effectiveness factor indicating the effectiveness of the security infrastructure in increasing the security level of each firm. Firms also invest in disaster recovery measures to limit the impact of successful attacks against them.

Disaster Limitation Level

$$g = \left(1 - k_{g}\right)(1-B)T \tag{2.6}$$

where, k_{g} is the disaster recovery effectiveness factor that defines how effective are the backup technologies in reducing the damage level of each firm.

2.3.2 Criminals

Criminals have one decision variable:

Variable: Activity Level, $A \in [0,1]$ and is continuous and independent

Criminals have to decide how much criminal activity to indulge in order to cause damage to firms' information systems. At the start of each period, each criminal has to decide on the activity level.

Each criminal also possesses a pre-defined skill level. The skill level of the criminal is defined as $\theta \in [0,1]$. The skill level classifies different criminals based on their capability to penetrate a firm's defenses. The skill level is a preset random variable for each criminal. Criminals do not acquire new skills or loose any skills during the progression of the economy.

Once criminals have made the decision on the activity level for the period, the costs of the effort to each criminal are computed.

Effort cost:

$$E = aA^2 \tag{2.7}$$

2.3.3 Environmental Variables

Apart from the decisions made by the agents, there are some environmental variables that are externally determined and are preset for specific experiments. The values of these environmental variables are defined by the research team and govern different economic states in the agent-based economy. The summary of these environmental variables is given in Table 2.1.

Table 2.1: Environmental Variable

Parameter	
v	Technology value parameter
t	Technology infrastructure cost parameter
s	Security infrastructure cost parameter
b	Backup resource cost parameter
k_ψ	Security effectiveness parameter
k_g	Disaster recovery effectiveness parameter
l	Law enforcement activity level
f	Punishment level to the criminals if caught
γ	Criminal gain parameter

2.4 Agent Interactions and Economy Progression

Once the agents have made their investment decisions for the period, the agents are inserted into a common artificial environment where the two types of agents can interact with each other. Once a criminal is matched against a firm, the criminal chooses whether or not to attack the firm.

If a criminal j chooses a firm i to attack, the probability that the attack will be successful is given by,

$$\rho_{ij} = \frac{1}{k_{\psi}} \theta_j A_j (1 - S_i) \tag{2.8}$$

If the above attack against the firm is successful then the firm suffers damages while the attacker gains benefits. The damage to the firm i from an attack from criminal j is given by,

$$d_{ij} = k_d \theta_j A_j \frac{g_i}{\psi_i} \tag{2.9}$$

The gain of the criminal j from a successful attack on firm i is given by,

$$G_{ij} = \gamma d_i \tag{2.10}$$

However, even if the criminal is successful in exploiting the vulnerabilities of a firm's information infrastructure, there is a chance that the criminal could get caught as a result of the firm's security infrastructure and law enforcement activity. If a criminal j attempts to perpetrate an illegal activity against a firm i, the probability that the criminal gets caught and convicted is given by,

$$\lambda_{ij} = (1 - \theta_j) A_j S_i l \tag{2.11}$$

If the criminal is caught and faces punishment, the punishment to the criminal i resulting from an attack on firm j is given by,

$$F = f d_{ij} \tag{2.12}$$

where, f is the punishment level determined by the government.

2.4.1 Updating Wealth at the end of each period

At the end of each period, the change in wealth of both firms and criminals is updated. Let, Π_X represent the wealth of a firm at the end of a period X. The change in the net value of the firm i for period X is given by $\Delta\Pi_X$:

1. If the attack against the firm was unsuccessful or if the firm was not attacked,

$$\Delta\Pi_X = V_i - C_{1i} - C_{2i} - C_{3i} \tag{2.13}$$

2. If the attack against the firm was successful,

$$\Delta\Pi_X = V_i - C_{1i} - C_{2i} - C_{3i} - d_{ij} \tag{2.14}$$

The total value to the firm at the end of period X is given by,

$$\Pi_X = \Pi_{X-1} + \Delta\Pi_X \tag{2.15}$$

Let, Γ_X represent the net gain of the criminal at the end of a period X. The change in the net value of the criminal j for period X is given by $\Delta\Gamma_X$:

1. If the attack against the firm was unsuccessful and the criminal is not caught,

$$\Delta\Gamma_X = -E_j \tag{2.16}$$

2. If the attack against the firm was successful and the criminal is not caught,

$$\Delta\Gamma_X = G_{ij} - E_j \tag{2.17}$$

3. If the criminal is caught and punished,

$$\Delta\Gamma_X = -E_j - F_{ij} \tag{2.18}$$

The net gain to the attacker at the end of period X is given by,

$$\Gamma_X = \Gamma_{X-1} + \Delta\Gamma_X \tag{2.19}$$

2.4.2 Updating the Decisions for the next period

The agents update their decisions every period. The change in the decision depends on the decisions and performance of the agents in the current period.

Firms update their technology infrastructure, security infrastructure and backup resources in response to the success or failure of the attacks and the magnitude of the damage suffered. Let, τ, σ and β represent the fractional changes in technology infrastructure, security infrastructure and backup resources respectively. The changes in the decisions for different scenarios are:

1. If the firm is not attacked by criminals or the attack is unsuccessful and hence the firm suffers no damages.

$$\Delta T_X = \tau' T_X \tag{2.20}$$

where, $\tau' \in (0,1)$ indicates a slight increase in the technology infrastructure of the firm as the firm believes it can increase its technology level to get more benefits.

$$\Delta S_X = \sigma' S_X \tag{2.21}$$

where, $\sigma' \in (-1,0)$ indicates a slight decrease in the security infrastructure of the firm. In this scenario, the firm finds it more beneficial to save financial resources.

$$\Delta B_X = \beta' B_X \tag{2.22}$$

where, $\beta' \in (-1,0)$ indicates a slight decrease in the backup resources of the firm. In this scenario, the firm finds it more beneficial to save financial resources.

2. If the attack against the firm is successful and the firm suffers either no or some damage.

$$\Delta T_X = \tau'' d_i \tag{2.23}$$

where, $\tau'' \in (-1,0)$ indicates that the firm reduces its technology infrastructure in response to exploitation of technology vulnerabilities by the criminals.

$$\Delta S_X = \sigma'' d_i + \sigma''' \tag{2.24}$$

where, $\sigma'', \sigma''' \in (0,1)$ indicates that the security infrastructure in the previous period was not enough and the firm needs to increase the security infrastructure to counter the attacks from the criminal. The increase in security has two components: the first is proportional to the damage suffered and the second takes into account the failure of the current security infrastructure in preventing the attack.

$$\Delta B_X = \beta'' d_i \tag{2.25}$$

where, $\beta'' \in (0,1)$ indicates that the firm was not able to limit the damage in the previous period and it needs to increase the disaster limitation levels.

The technology, security and backup infrastructures of the firm are now defined as:

$$T_{X+1} = T_X + \Delta T_X$$
$$S_{X+1} = S_X + \Delta S_X \quad (2.26)$$
$$B_{X+1} = B_X + \Delta B_X$$

Criminals update their activity level as a result of their performance in the past period. Let, α represent the fractional change in attacker activity levels in response to the performance in the current period. The changes in activity level for different scenarios are:

1. If the criminal is caught and is punished

$$\Delta A_X = \alpha' F_j \quad (2.27)$$

where, $\alpha' \in (-1,0)$ indicates a decrease in the activity level of the criminal as the attacker becomes more cautious as a result of being caught and punished.

2. If the criminal is not caught but is successful

$$\Delta A_X = \alpha'' A_X \quad (2.28)$$

where, $\alpha'' \in (0,1)$ indicates a slight increase in the activity level of the criminal as the criminal becomes more confident of and indulges in even more criminal activity.

3. If the criminal is not caught and the attack is not successful

$$\Delta A_X = \alpha''' A_X \quad (2.29)$$

where, $\alpha''' \in (0,1)$ and $\alpha''' > \alpha''$ indicates an increase in the activity level of the attacker increases in an attempt to be successful in the next period.

2.5 Experiment Design

We conducted several experiments with the agent-based economy to determine what strategies were more successful in different environmental conditions. We implemented two agent interaction mechanisms in the environment. These interactions define how criminals choose the target. These interactions are:

1. Criminals choose the firms randomly
2. Criminals prefer to attack the firms with higher technology levels

The first sets of hypotheses are related to firms' decisions and the effect of the interactions on the firms' performance.

Firms can be distinguished based on two criteria:

1. The initial setting of the firm, i.e. what were the initial levels of technology infrastructure, security infrastructure and backup resources of the firm. These scenarios would help us evaluate the question:

   Do the initial technology infrastructure, security infrastructure and backup resources of the firm has an impact on the performance of the firm, or does the firm rebound and perform equally well compared to other firms?

For the purpose of analysis we assume two different levels of technology infrastructure, security infrastructure and backup resources. We distinguish these levels to be low and high levels of each decision variable with the setting for low and high levels being derived from two different uniform distributions. The possible combinations of initial settings are described in Table 2.2.

Table 2.2: Different Classes of firms

Class	Technology	Security	Back Up
Firm I	High	High	High
Firm II	High	High	Low
Firm III	High	Low	High
Firm IV	High	Low	Low
Firm V	Low	High	High
Firm VI	Low	High	Low
Firm VII	Low	Low	High
Firm VIII	Low	Low	Low

The above different firm types can be tested using 2 X 2 X 2 factorial design with technology, security and backup as three factors. Each of these factors can actually take 2 values: high and low. The above design has 3 main effects: technology, security and

backup resources respectively; 3 two-way interactions: technology-security, security-backup resources and technology-backup; and 1 three-way interaction: technology-security-backup resources.

The hypotheses that are going to be addressed by the above design are presented below. Each of these hypotheses is stated as a null hypothesis.

H1: *There is no difference in the performance of different types of firms.*

H2: *There is no technology main effect present i.e. the level of technology does not affect the performance of the firm.*

H3: *The level of security does not affect the performance of the firm.*

H4: *The level of backup resources does not affect the performance of the firm.*

H5: *There are no technology and security interaction effects present.*

H6: *There are no technology and backup interaction effects present.*

H7: *There are no backup and security interaction effects present.*

H8: *There are no three way interaction effects between technology, security and backup resources are present.*

2. The second classification of firms deals with their behavior. We analyze two different behavior types or personalities of a firm – aggressive firms and cautious firms. Aggressive firms are the firms that show greater reaction to the events in the economy; i.e. if the firm is attacked and it suffers damages, the aggressive firm will drastically increase the security and backup levels. On the other end, the cautious firms are much more watchful in their reaction and change their decisions by only small amounts.

The hypothesis that is going to be evaluated to measure the effects of the firm personality is:

H9: *There is no difference in the performance of firms with different personality types.*

Criminals can be distinguished based on their skill levels and the initial activity level. These scenarios would help us answer the question:

Does it help for the highly skilled criminal to be aggressive in attacks or is it better to take a cautious approach?

Based on skill level and initial activity level of criminals we get four different types of criminals. These classes are defined in Table 2.3.

Table 2.3: Classes of Criminals

Class	Skill Level	Initial Activity Level
Attacker I	High	High
Attacker II	High	Low
Attacker III	Low	High
Attacker IV	Low	Low

The above classification of criminals can be evaluated using a 2X2 factorial design. The two factors in the design are the criminal skill level and the initial activity level. Each of these factors can take two levels: high and low. There are two main factors in the design, skill level and the activity level, and one interaction effect, skill level- activity level.

The hypotheses that address the agent performance are defined below:

H10: *There is no difference in the performance of different types of criminals.*

H11: *The activity level of the criminal does not affect the net gains to the criminal.*

H12: *The skill level of the criminal does not affect the net gains to the criminal.*

H13: *There are no interaction effects present between the activity level and the skill level.*

We also evaluate the performance of the agents in different environmental conditions. These environmental conditions govern different market conditions that influence the price and the value of the technology infrastructure, security infrastructure and backup resources. These conditions also control the technological environment that

influences the effectiveness of the security and backup technologies. The legal environment governs the level of the punishment to the criminals if they are caught. We evaluate each of the environmental conditions for two different settings by providing two contrasting scenarios for each of them. The evaluated environmental variable are presented in Table 2.4.

Table 2.4: Environmental Settings

Variable	Values	
k_{ψ}	High	Low
k_{g}	High	Low
f	High	Low

The hypotheses for the environmental variables are:

H14: *There is no difference in the performance of firms for different settings of the environmental variables.*

H15: *There is no difference in the performance of firms for changes in effectiveness of security.*

H16: *There is no difference in the performance of firms for changes in effectiveness of backup.*

H17: *There is no difference in the performance of firms for changes in punishment level.*

H18: *There are no interaction effects between effectiveness of security and effectiveness of backup.*

H19: *There are no interaction effects between effectiveness of security and a positive fine.*

H20: *There are no interaction effects between effectiveness of backup and a positive fine.*

H21: *There are no interaction effects between effectiveness of security, effectiveness of back and a positive fine*.

We conduct multiple sets of experiments for different scenarios and evaluated the results. The statistical testing and analysis of the hypotheses and the results are presented in the next section.

2.6 Results and Discussion

We conducted several sets of experiments under different settings. Each population of firm agents was populated with an equal number of agents for each class. Similarly, each population of criminal agent was populated with equal numbers of each attacker agent class. We conducted several experiments for different combinations of firm number and criminal number in the population. 10 experiments were conducted for each setting and each experiment was conducted for 500 periods. The data collected was used for analysis in our research hypotheses.

H1: *There is no difference in the performance of different types of firms*.

We conducted a three-factor ANOVA analysis for the performance of a firm against technology, security and backup resources to address H1 to H8. Table 2.5 shows the ANOVA results for Technology, Security and Backup for different combinations of firm and criminal numbers. The results show that hypothesis H1 was rejected for all the combinations indicating that the there is a difference between the performance of different types of firms when firms are classified based on the level of their technology, backup and security infrastructure. We further analyze the effects of technology, security and backup infrastructure through hypotheses H2 to H8.

Table 2.5: ANOVA results for Technology, Security and Backup

Number of Criminals	64	128	128	128	256	256	256
Number of Firms	128	64	128	256	64	128	256
Overall Model	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Technology	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Security	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Backup	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Technology-Security	0.1396	<0.001	<0.001	0.2243	<0.001	<0.001	<0.001
Technology-Backup	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Security-Backup	0.1368	0.0830	0.0306	0.0706	0.3883	0.5215	0.0839
Technology-Security-Backup	0.8685	0.5235	0.8225	0.0708	0.5363	0.2259	0.2002

H2: *There is no technology main effect present i.e. the level of technology does not affect the performance of the firm.*

H3: *The level of security does not affect the performance of the firm.*

H4: *The level of backup resources does not affect the performance of the firm.*

It can be seen from Table 2.5 that H2 was rejected for all firm-criminal combinations indicating that level of technology infrastructure affected the performance of the firms. This is an expected result since organizations derive benefits from technology. Firms with higher technology perform significantly better than firms with the lower technology. This result indicates that in the long run the value of technology infrastructure far exceeds the damages suffered due to vulnerabilities in firms' resources and firms should look to invest in technology infrastructure despite the threat from criminal elements.

The hypotheses H3 and H4 were also rejected for all firm-criminal combinations indicating the presence of both security and backup main effects. Further analysis of the firm performance in response to level of security infrastructure indicated that firms with higher security infrastructure performed better than those with lower levels of security

infrastructure for all but two firm-criminal combinations. In the cases where the number of firms in the environment far exceeded the number of criminals, the performance of firms was inversely correlated with the security infrastructure. This result indicates that in the scenarios where the number of criminals is low, the threat to firms' resources is not significant enough to warrant investment in security infrastructure. In such scenarios, it is much more beneficial for firms to absorb the damages suffered in case of successful attack. This is an interesting result that discourages the firms from making investment in security technologies when there are not enough criminals in the environment. The above result has public policy implications for law enforcement agencies to come up with ways to discourage the criminals and reduce the number of criminals in the environment. Analysis of firm performance in response to level of back infrastructure indicated that the firms with lower backup infrastructure performed better than the firms with higher backup infrastructure. This result indicates that the investment in backup infrastructure does not limit the damages enough to justify the cost of backup infrastructure. The firms are better off increasing the security infrastructure to reduce the probability of successful attacks compared to attempts to limit the damage suffered from successful attacks by increasing the backup infrastructure. The above two results indicate that the firms can not undermine the importance of security in most scenarios and it is prudent for firms to invest in security technologies to prevent successful offenses against their information system resources. We further test the interaction effects between, technology, security and backup infrastructure through hypotheses H5 to H8.

H5: *There are no technology and security interaction effects present.*

H6: *There are no technology and backup interaction effects present.*

H7: *There are no backup and security interaction effects present.*

H8: *There are no three way interaction effects between technology, security and backup resources are present.*

Table 2.5 indicates that hypothesis H5 is rejected for all firm-criminal combination but for the cases where the number of firms far exceeds the number of criminals. The rejection of H5 indicates the presence of technology-security interaction effects for those cases. For the cases where the number of firms exceeds the number of

criminals, the interaction effects are not present indicating that relative levels of technology and security infrastructure do not influence the firms' performance. This is an interesting finding that shows that firms should not protect their technology investments by investing in security. The intuition behind this is that when there is less number of criminals in the environment, the threat of damage from the criminals does not rise as fast as the increase in costs of security. Further, if it is possible through public policy to decrease the number of hackers and other perpetrators in the environment, the overall risks to organizations reduces therefore enabling the organizations not to invest in security. The hypothesis H6 was rejected for all firm-criminal combinations indicating the presence of correlation between technology infrastructure and backup infrastructure of the firms. However, we failed to reject hypotheses H7 and H8 for all firm-criminal combinations. This indicates that there was no significant evidence of correlation between security infrastructure of the firms and the backup infrastructure of the firms. Also, no three-way interactions between technology, security and backup infrastructure were present. We further analyze the performance of the firms based on their personality type through hypotheses H9.

H9: *There is no difference in the performance of firms with different personality types.*

We performed a single factor ANOVA on the performance of the firm for the two different personalities of the firm, i.e. the aggressive and cautious firms. The analysis of the results helped us to address the hypothesis H9. The results are presented in Table 2.6.

Table 2.6: ANOVA results for Personality

Number of Criminals	64	128	128	128	256	256	256
Number of Firms	128	64	128	256	64	128	256
Personality	0.5622	0.9019	0.9551	0.6321	0.6013	0.6719	0.8325

Table 2.6 indicates that we failed to reject hypothesis H9 for all combinations of number of firms and number of criminals. This indicates that we did not have significant evidence that either aggressive or cautious firms outperform the other significantly. The firms that took cautious approach to investment in security infrastructure did not perform significantly worse than the firms that more aggressively responded to criminal activities by increasing the security infrastructure quickly. This indicates that as long as the firms invested in security, over the long run they were able to secure their resources and were able to recover the losses. The aggressiveness and the timing of the security investments did not have much influence on the long-term performance of the firms. We further analyze the performance of different type of criminals through hypotheses H10 to H13.

H10: *There is no difference in the performance of different types of criminals.*

We performed a two-factor ANOVA for criminals' net gains against the activity level and the skill level of the criminal. Table 2.7 presents the results from the ANOVA. Hypothesis H10 was rejected for all firm-criminal combinations indicating that there is a difference in the performance of different types of criminals when criminals are classified based on their activity level and skill level. We further analyzed the affects of activity level and skill level through hypotheses H11 to H13.

Table 2.7: ANOVA results for criminal Activity and Skill

Number of Criminals	64	128	128	128	256	256	256
Number of Firms	128	64	128	256	64	128	256
Overall Model	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Activity	0.0058	0.0004	0.0055	0.0015	<0.001	<0.001	0.5252
Skill	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Activity-Skill	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001

H11: *The activity level of the criminal does not affect the net gains to the criminal.*

H12: *The skill level of the criminal does not affect the net gains to the criminal.*

H13: *There are no interaction effects present between the activity level and the skill level.*

Table 2.7 indicates that hypothesis H11 was rejected for all but one cases. For the case of large number of criminals and large number of firms there was no significant evidence that either high activity or low activity criminals outperformed the other. For all other cases, the activity level of the criminal determined the performance of the criminal. However, upon closer inspection it was found that the criminals with lower activity levels actually outperformed the criminals with higher activity levels. The result is somewhat consistent with our theoretical predictions in the first essay that indicate that it is prudent for criminals to decrease the activity level if they have a certain minimum set of skills. Hypothesis H12 was rejected for all firm-criminal combinations. This indicates that skill level of the criminals influenced their performance. Criminals with higher skill levels performed consistently better than the criminals with lower skill levels. The results indicate that while the criminal can increase its chances of success by increasing its activity level, the benefits from raising the activity level do not rise as fast as the risk of getting caught and punished. However, by raising the skill level and reducing its activity level, the criminal is able to increase the probability of success while reducing or

maintaining the same level of risk of getting caught. Hypothesis H13 was also rejected indicating that there was some correlation present between the activity level of criminals and the skill level of criminals. We analyze the performance of firms in response to environmental variables through hypotheses H14 to H21.

H14: *There is no difference in the performance of firms for different settings of the environmental variables.*

We performed a three-factor ANOVA on firm performance for three environmental variables to test hypotheses H14 to H21. These environmental variables are: effectiveness of the security technologies, effectiveness of the backup resources and the punishment level to the criminals. Table 2.8 presents the ANOVA results. From the ANOVA table it is clear that the hypothesis H14 is rejected and the level of environmental variables has a significant effect on the performance of firms. We further analyze the effects through hypotheses H15 to H21.

Table 2.8: ANOVA results for Effectiveness of Security, Effectiveness of Backup Resources and Fine

Number of Criminals	64	128	128	128	256	256	256
Number of Firms	128	64	128	256	64	128	256
Overall Model	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Effsec	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Effback	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001	<0.001
Fine	0.9380	0.4461	0.8944	0.0419	0.2848	0.3029	0.5804
Effsec-Effback	0.9355	0.1506	0.1385	0.9705	0.3382	0.8077	0.5071
Effsec-Fine	0.4004	0.6148	0.7565	0.0244	0.6619	0.9707	0.4596
Effback-Fine	0.9021	0.3092	0.7748	0.1086	0.8666	0.5382	0.8262
Effsec-Effback-Fine	0.7617	0.8022	0.5208	0.4864	0.5922	0.2671	0.8778

H15: *There is no difference in the performance of firms for changes in effectiveness of security.*

H16: *There is no difference in the performance of firms for changes in effectiveness of backup.*

H17: *There is no difference in the performance of firms for changes in punishment level.*

Hypotheses H15 and H16 were rejected indicated that effectiveness of security technologies and backup technologies influence the performance of the firms. The above results encourage more research in making security technologies more effective and efficient. If the effectiveness of both the security technologies and backup resources increase, the firms can achieve much higher level of security with same costs. Firm performance improves as the effectiveness of the security technologies increases. Firm performance also improves with the increase in effectiveness of backup technologies. The hypothesis H17 was rejected indicating that increase in punishment levels to the criminals does not affect the performance of the firms.

H18: *There are no interaction effects between effectiveness of security and effectiveness of backup.*

H19: *There are no interaction effects between effectiveness of security and a positive fine.*

H20: *There are no interaction effects between effectiveness of backup and a positive fine.*

H21: *There are no interaction effects between effectiveness of security, effectiveness of back and a positive fine.*

Hypotheses H18, H19, H20 and H21 were all rejected indicating the absence of any interaction effects, i.e. the variables effectiveness of security technologies, effectiveness of backup resources and punishment levels of the criminals are not correlated to each other.

2.7 Summary

The results of experiments conducted in an agent-based economy revealed some interesting outcomes, several of which were consistent with our findings in the first essay. The results indicate that security is effective in improving the performance of the firms. Interestingly, when the number of criminals in the environment was far fewer than the number of firms, the security became ineffective in improving the performance of the firm and only increased the costs to the firm. In such scenarios, the firm was better off absorbing the cost of any damage suffered as the risk of any such damage was low. The backup resources did not prove effective in limiting the damage to the firm and only ended up increasing the costs to the firm. The personality of the firm did not play any significant role in determining the performance of the firm. The findings also indicate improvement in the performance of firms when effectiveness of the security and backup technologies increases. However, the increase in fine did not prove to be a deterrent to the criminal and the performance of the firm did not improve in response to increase in the punishment level to criminals.

From the criminal's point of view, the findings indicate that skilled criminals performed consistently better. The performance of criminals suffered when they increased their activity level indicating the increased risk of getting caught and convicted. This might be consistent with one of the theoretical findings that indicate that criminals should decrease their activity level if they possess a certain set of skills.

These experiments were conducted with little intelligence in the agents. Agent decisions were modified as a fixed set of rules with no learning involved. It would be interesting to explore the learning of agents in such an environment where agents learn from their past performance and change their behavior adaptively. This would also give an indication whether firms learn from their past mistakes or are able to recover from initial setbacks. In the future, we plan to implement both learning in the behavior of the agents and experience as a parameter.

3 GENETIC ALGORITHM BASED APPROACH FOR MATCHING SECURITY PROFILES TO VULNERABILITIES

3.1 Introduction

In recent years information technology has developed into an essential infrastructure resource for organizations. An increasing number of organizations are investing in information technology to support business operations and gain strategic advantages. These information systems possess weaknesses or vulnerabilities that could provide unauthorized access to information stored in them. Entities such as hackers, terrorists and business competitors, are on the lookout for any vulnerability in the information systems of organizations and seek to exploit these weaknesses for psychological, political or competitive advantages. These entities are a serious threat to organizational information systems and create financial and reputation implications for the organizations.

Organizations hope to prevent unauthorized access to their systems by using security technologies that address the vulnerabilities present in information systems. However, each security technology only addresses specific vulnerabilities and could create other vulnerabilities. Organizations also have to take into account the cost of using each security technology. Thus it is always a difficult decision for organizations to choose a security profile that addresses as much vulnerability as possible while trying to minimize the cost of the profile.

In this paper, we present and evaluate a Genetic Algorithm based approach that would enable organizations to choose a minimal cost security profile that provides maximal vulnerability coverage. Furthermore, we will compare the GA approach to the exploratory approach of evaluating all possible security profiles. We will perform these

evaluations for several combinations and sizes of vulnerability matrices and security profiles.

3.2 Genetic Algorithms for Multi-Objective Optimization Problems

Our problem is a multi-objective in nature since we are trying to evolve security profiles to achieve two objectives: to minimize the exposed vulnerabilities of the organizations and to minimize the cost of security used to address the vulnerabilities. Genetic Algorithms have been successfully used for searching, single objective optimization or for machine learning. Goldberg (Goldberg 1995) provides a general construction for Genetic Algorithm and how they can be designed and implemented for solving single optimization problems. Over the years researchers have found techniques to expand the application of Genetic Algorithms to multi-objective problems. Coello (Coello 2000) provided a survey of different GA based techniques for solving multi-objective optimization problems. The first approach involved combining multiple objectives into one objective using addition, multiplication, or any other combination of arithmetical operations. Coello argued that if the combination of objectives is possible, this is not only one of the simplest approaches but also one of the most efficient ones.

Syswerda et al (Syswerda and Palmucci 1991) used a weighted combination of fitness functions to add or subtract values during the schedule evaluation of a resource scheduler, depending on whether or not the constraints were violated. Jakob et al (Jakob, Gorges-Schleuter et al. 1992) implemented a weighted sum of objectives approach in a task planning problem to move the tool center point of an industrial robot to a given location as quickly and as precisely as possible. Yang and Gen (Yang and Gen 1994) utilized the weighted objective technique to solve a bicriteria linear transportation problem.

Charnes and Cooper and Ijiri (Charnes and Cooper 1961; Ijiri 1965) developed a genetic programming technique where decision makers have to assign targets or goals that they wish to achieve for each objective. These values are incorporated into the problem as additional constraints and the objective function tries to minimize the absolute

deviations from the targets to the objectives. Weinke et al (Wienke, Lucasius et al. 1992) used this approach to simultaneously optimize the intensities of six atomic emission lines to trace elements in alumina powder. Sandgren (Sandgren 1994) used genetic programming to optimize plane trusses and the design of planar mechanism. Ritzel et al (Ritzel, Eheart et al. 1994) presented an $\varepsilon-$constraint approach that optimizes one objective function while considering other objective functions as constraints bound by some allowable levels of ε_i. Loughlin (Loughlin and Ranjithan 1997) applied this technique to a real-world air quality management problem with conflicting objectives of minimizing the cost of controlling air pollutants and maximizing the amount of emissions reduction.

In this paper we utilize the weighted sum of objectives technique to combine the conflicting objective of minimizing the security costs of addressing vulnerabilities and maximizing the number of vulnerabilities covered. The problem with this approach is that it requires some information regarding the range of weights (Coello 2000). However, in our problem a good estimate on the weights of the objectives can be made based on the type and preferences of the organization. Organizations such as financial institutions, for which covering vulnerabilities is critical, will put more emphasis on maximizing the number of vulnerabilities covered, while the organizations that don't need absolute security might want to minimize the cost of security.

3.3 Definition of Vulnerabilities and Securities

Organizational information systems have vulnerabilities that can be exploited by unauthorized sources. Organizations seek security technologies to try to address these vulnerabilities and try to minimize the risk to the organizations. RAND report (1999) identifies a set of generic vulnerabilities that most of the organizational information systems can have. These vulnerabilities are classified in seven different categories. Organizations can map their information systems to these vulnerabilities to assess the state of risk to their information systems. The list of vulnerabilities and the variables we represent them by in our model is presented in Table 3.1.

Table 3.1: Technology Vulnerabilities

Category	Vulnerability	Representation
Inherent Design/Architecture	Uniqueness	v_1
	Singularity	v_2
	Centralization	v_3
	Separability	v_4
	Homogeneity	v_5
Behavioral Complexity	Sensitivity	v_6
	Predictability	v_7
Adaptation and Manipulation	Rigidity	v_8
	Malleability	v_9
	Gullibility	v_{10}
Operation/Configuration	Capacity Limits	v_{11}
	Lack of Recoverability	v_{12}
	Lack of Self-Awareness	v_{13}
	Difficulty of Management	v_{14}
	Complacency/Co-optability	v_{15}
Indirect/Nonphysical Exposure	Electronic Accessibility	v_{16}
	Transparency	v_{17}
Direct/Physical Exposure	Physical Accessibility	v_{18}
	Electromagnetic Susceptibility	v_{19}
Supporting Facilities/Infrastructures	Dependency	v_{20}

Organizations invest in security techniques to address the vulnerabilities described above. The security technologies provide security by reducing the vulnerabilities, identifying attacks and reacting to these attacks. Each security technology addresses certain vulnerabilities directly by design; they reduce certain other vulnerabilities indirectly as a second order effect. However, security technologies can

also directly or indirectly create certain other vulnerabilities in the system. We present the generic security technologies described in the RAND report in Table 3.2. These generic security technologies have to be implemented in the context of the system and actual security technologies.

Table 3.2: Generic Security Technologies

Security	Representation
Heterogeneity	s_1
Static Resource Allocation	s_2
Dynamic Resource Allocation	s_3
Redundancy	s_4
Resilience and Robustness	s_5
Rapid Recovery and Reconstitution	s_6
Deception	s_7
Segmentation, Decentralization and Quarantine	s_8
Immunologic Identification	s_9
Self-organization and Collective Behavior	s_{10}
Personnel Management	s_{11}
Centralized Management of Information Resources	s_{12}
Threat/Warning Response Structure	s_{13}

Each of these security technologies addresses some of these vulnerabilities fully or partially and creates some vulnerability directly or indirectly. The mapping of these security technologies to vulnerabilities is presented in Table 3.3. If an organization is looking to cover its vulnerabilities by investing in security technologies – it has two major goals:

1. Minimize the number of uncovered vulnerabilities after implementation of security technologies. The emphasis here is to cover more critical vulnerabilities first.
2. Minimize the cost of security to achieve the first objective.

Achieving these two objectives is not easy since the organizations have to constantly make trade-offs between security costs and allowing some vulnerabilities to be uncovered. Malicious agents can exploit these uncovered vulnerabilities resulting in damages to the organization. In the next section we address the complexity of this problem.

Table 3.3: Matching Security to Vulnerabilities

		Security												
		s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}
Vulnerability	v_1			1		1	1			1	-1			
	v_2		1	1	1	.5	1	1	1		1			
	v_3		-.5			.5	1	1	1		1		-1	
	v_4		-1	1	1		1		-1		1			
	v_5	1			-1	.5			1				-.5	
	v_6	-1		-1		.5	1	-1	1	-1	-1			
	v_7	1		1				1	-1	1			-.5	
	v_8		-1						-1	1	1			.5
	v_9	1						1		1		.5		.5
	v_{10}			-1						1				.5
	v_{11}			-1										.5
	v_{12}			1	1	.5	1		1		1		.5	.5
	v_{13}									1		.5	.5	
	v_{14}	-1		-1				-1	1	-1	1	1	1	-.5
	v_{15}		.5			-.5		-1	1	1	-.5	1		1
	v_{16}		1	1				1	1	1		.5		1
	v_{17}							1						1
	v_{18}		1	1	1	1	1	1	1			.5		1
	v_{19}	1	1		1	1	1	1	1					.5
	v_{20}	1		1	1	1			1		1		-.5	.5

1	Security directly addresses vulnerability
.5	Security indirectly addresses vulnerability
-.5	Security indirectly creates vulnerability
-1	Security directly creates vulnerability

3.4 Complexity of the problem

In this section, we will demonstrate that our objective of trying to cover all vulnerabilities while minimizing security costs and residual vulnerabilities is a generalization of the well-known set-covering problem. According to Coreman (Cormen, Leiserson et al. 2002) a set-covering problem is defined as

> Set-covering consists of a finite set X and a family F of subsets of X, such that every element of X belongs to at least one subset in F.

From an optimization standpoint, the objective of a set-covering problem is to find the minimal subset in F such that the selected subset contains all the elements of X. We can also map the set-covering problem into graphs. Imagine that each element of the set X is represented by edges in the graph and each of the vertexes in the graph represents a subset that contains some edges in the graph; i.e. the edges are connected to the vertex. The objective of the set-covering problem is now to find the minimum number of vertices that cover all the edges in the graph. The union of the subsets represented by each vertex gives us the minimal subset that contains all the elements of set X. It has been shown by the researchers that the set-covering problem is NP-complete.

The objective of the vulnerability-covering problem is to maximize the number of vulnerabilities covered while minimizing the cost of security technologies. However, implementation of security also results in some new vulnerabilities. We will call these residual vulnerabilities. The problem now can be newly defined:

> If we have a set of vulnerabilities V and a set of security technologies S whose subsets cover some elements in set V, but also result in creating some subset of residual vulnerability set R then the problem is to find the minimal subset of S that covers all elements in V while having the smallest resulting subset of R.

Representing the above problem through graphs, let each unique vulnerability in set V be represented by a colored edge. Each color represents a unique vulnerability. Let each vertex in the graph represent distinct security technologies from set S. Each security technology that covers vulnerability will have an edge with that color on the