Founded 1905

Economics of Information Security

- Impact of Government Enforcement on Hackers' Behaviors

- An Event Study Analysis

Wang Chenyu

A THESIS SUBMITTED

FOR THE DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF INFORMATION SYSTEMS

SCHOOL OF COMPUTING

NATIONAL UNIVERSITY OF SINGAPORE

2007

Abstract

Information security deals with the protection or preservation of six key aspects of information, namely, confidentiality, integrity, availability (CIA), authenticity, accountability, and non-repudiation. Considering organizations' ever-increasing dependence on information systems for operational, strategic, and e-commerce activities, protecting information systems against potential threats to the organization has become a major concern for governmental policy as well as business corporations. In this paper, an extensive literature review of information security background, barriers to sound information security, and traditional measures to address information security are presented to serve as a solid foundation for further researches. The pros and cons of each method introduced are analyzed. Besides, this paper makes a meaningful attempt to establish an empirical econometric model in order to investigate the effect of government enforcement on hackers' behaviors using event study methodology. In addition, panel data estimation (specifically, the fixed effects model) is also employed to further illustrate the results given by the event study analysis. Our results demonstrate that government enforcement has a significantly negative and deterrent impact against hackers' behaviors by dramatically reducing the number of security attacks committed either for an individual country or at a global level. It complements the existing body of research in the realm of information security by incorporating an important variable - *government enforcement* - and contributes, to some degree, to the establishment of a more sophisticated model of information security. In addition, our results also provide valuable policy as well as economic implications.

KEYWORDS: Information Security, Government Enforcement, Efficient Market Hypothesis (EMH), Denial-of-Service (DoS), Capital Asset Pricing Model (CAPM), Event Study Methodology, Event Window, Estimation Window, Cumulative Abnormal Return (CAR), Panel Data, Fixed Effects Model (FEM), Random Effects Model (REM), Free/Open Source software (F/OSS).

Acknowledgement

First and foremost, I would like to extend my deepest gratitude to my supervisor, Prof. Png Paak Liang, Ivan, for instructing me throughout the whole research. Prof. Ivan has been very patient in guiding me to identify the research question, construct and revise the model, collect data, and conduct empirical analysis. This study would be impossible without his contributions and guidance.

Second, I greatly appreciate the invaluable feedback and comments provided by my GRP reviewers - Dr. Goh Khim Yong and Dr. Atreyi Kankanhalli. Their professional and insightful advice has no doubt greatly improved and clarified this research work.

Third, I am also indebted to many of my seniors who have willingly and patiently addressed my questions and provided me with many precious comments and suggestions.

Finally, I would like to express my sincerest thanks to my parents for their love, support, and encouragement to help me grow and advance during all these years of my life.

List of Figures and Tables

Table of Contents

Chapter 1 Introduction

1.1 Background and Motivation

In the current ICE (Internet Changes Everything) Age, there is a growing consensus that information technology (IT), especially the Internet, is altering the way we live, work, communicate, and organize our activities (Laudon and Laudon, 2005). The Internet has provided companies as well as individuals with tremendous economic benefits, including dramatically reduced costs and enhanced productivity. However, the use of the Internet has also significantly increased potential vulnerabilities of organizations to a stream of new threats such as viruses, worms, hackers, information thefts, disgruntled employees, etc (Gordon and Loeb, 2002). According to a 2002 survey conducted by the Computer Security Institute and the Federal Bureau of Investigation (CSI/FBI), 90% of the respondents detected computer security breaches within the last twelve months and the average loss was estimated to be over $2 million per organization (Power, 2002). Besides, a 2005 CSI/FBI survey also revealed that website incidents had increased radically and that virus attacks remained to be the source of the greatest financial losses (Gordon et al., 2005). Other slightly informal surveys by Ernst & Young point out that 75% of businesses and government agencies have suffered a financial loss due to security breaches, 33% admit the lack of capability to respond, and nearly 34% of the institutions are incapable of identifying security threats within the organization (Insurance Information Institute, 2003). The terrible information security situation is also highlighted by Symantec Internet Security Threat Report (2005) - the number of new bot[1] variants remains to climb. For example, referring to Figure 1.1, in the current period, 6,361 new variants of Spybot[2] are reported to Symantec, which is a 48% increase over the 4,288 new variants documented in the second half of 2004. In addition, many high profile

[1] Bots are programs that are covertly installed on a user's computer in order to allow an unauthorized user to control the computer remotely.

[2] Spybot is one common form of bots, which is known to exploit security vulnerabilities.

corporations such as Microsoft, eBay, and Amazon.com have suffered large-scale denial-of-service (DoS) attacks, causing these companies inaccessible for a significant period of time (Gohring, 2002). Furthermore, some crackers have deliberately tarnished the websites of the Federal Bureau of Investigation (FBI), the Department of Defense (DoD), and the U.S. Senate (Vogel, 2002). But to make matters worse, the actual situation may be even worse. Based on several reports, many of the companies are reluctant to report security breaches to shareholders due to potential negative reputation and publicity, and the security breaches estimated might be the tip of a very large iceberg.

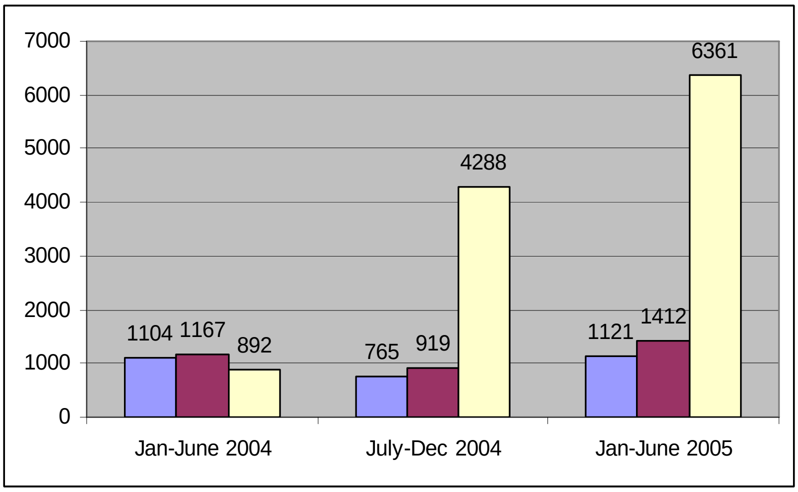

Figure 1.1: The Number of New Bot Variants

Considering the pervasive Internet risks discussed above and organizations' ever-increasing dependence on information systems for operational, strategic, and e-commerce activities, protecting information systems against potential threats to the organization has become a critical issue in handling information systems. In other words, information security is a crucial issue of and major concern for governmental policy as well as business corporations (Whitman, 2003). Information security is not only an enabler of business, but also a critical part of organizations. Continuous information security maintenance is the lifeblood of organizations especially in the current ICE Age (Dhillon, 2006). And the preservation of confidentiality, integrity, and availability of information from both internal and external threats within the organizations is vital to the successful operation of the businesses as well as governments. Accordingly, it is urgent and essential that organizations take strict measures to establish information security policies and procedures that adequately reflect the organizational context and new business processes so as to guarantee the successful functioning of the organizations.

Given the adverse situation of information security, the chief information security officers (CISO) of organizations are making non-trivial investments in information security to help safeguard their IT assets from security breaches. Besides, expenditures on investment in information security by institutions has been on the rise with an annual rate of 17.6% and the amount is predicted to approach $21.6 billion in 2006 (AT&T, 2004). However, the outcome is far from satisfactory and information security level has never improved (Whitman, 2003). Therefore, it is natural for scholars and practitioners to seek to address the following issue concerning information security: "What factor or factors have an effect on hackers' behaviors?". However, from the perspective of social research, it is almost impossible to answer such "what" question correctly and perfectly, since incorporating every aspect about the determinants poses a huge task for the researchers. Our paper tries to tackle the problem by proposing a specific research question as follows.

Information security is an issue of important concern to organizations as well as governments, and many researchers have been engaging in this dynamic and promising field. However, while prior researches provide important insights into the behaviors of various parties in the field of information security, nearly none of them directly focuses on the effect of government enforcement or even touch this area. The goal of our paper is to fill this void by focusing on one factor that has been, to the best of our knowledge, untouched yet in former researches and shedding light on the following research question: "What is the impact of government enforcement against hackers' behaviors?". This question spawns two streams of research: (1) Whether government enforcement encourages or discourages hackers to launch malicious attacks on the victims, and 2) Is there any significant effect of government enforcement on hackers' behaviors.

In this paper, we address the effect of government enforcement against hackers' behaviors by employing event study methodology - an approach widely used in finance and economics. We first adapt event study analysis to our situation, then conduct it for every country in the country list, and assess the respective effect within each country. Our results suggest that government enforcement has a significantly negative and deterrent impact against hackers' behaviors by dramatically reducing the number of security attacks launched by other hackers, which has important implications for policy making that deals with information security.

1. 2 Organization of the Paper

The remainder of this paper is organized as follows. Chapter 2 gives formal definitions of information security, introduces interacting agents, and presents barriers to sound information security. In Chapter 3, an extensive literature review is conducted on traditional measures to address information security issues with emphasis on behavioral aspects and economic approaches. The Pros and cons of each method are also analyzed. Some meaningful researches are identified and empirical results are analyzed in detail in Chapter 4 using both event study methodology and panel data estimation (the fixed effects model). Chapter 5 wraps up our discussion with a summary and concluding remark. Appendix A provides a list of countries' abbreviations. Appendix B shows the detailed list of events for the eight countries under investigation.

The objective of this paper is to review the field of information security as the groundwork for further research and serve as a guide for the solution of problems that have not been addressed. In addition, we will also conduct an empirical analysis with real-world data to investigate the effect of government enforcement against hackers' behaviors using both event study methodology and panel data estimation.

Chapter 2 Information Security

2.1 Formal Definition

Information security is by no means a new and innovative concept, and the need to safeguard information against malicious attacks is as old as mankind (Hoo, 2000). Currently, information security has changed from the preservation of physical locations and hardware to the inclusion of soft-side aspects such as information, data, etc.

What is Information Security

The definition of information security used here is adopted from the concept formulated by National Institute of Standards and Technology (NIST, 1995). Information security deals with the protection or preservation of six key aspects of information, namely, **confidentiality, integrity, availability (CIA), authenticity, accountability, and non-repudiation**.

Confidentiality: Confidentiality is defined as the protection of private data and the prevention of disclosure or exposure to unauthorized individuals or systems. Confidentiality is aimed at ensuring that only those with authorized rights and privileges to access information are able to perform so, and that those without are prevented from accessing it. When unauthorized users can have the access to the information, confidentiality is endangered and breached.

Integrity: Integrity means the prevention of unauthorized modification of information, and the quality or state of being whole, complete, and uncorrupted. This indicates that only authorized operators of systems can make modifications. The integrity of information is at stake when it is exposed to corruption, damage, destruction, or other disruption. Confidentiality and integrity are two very different concepts. In terms of confidentiality, the question is usually posed as “Has the data been compromised”. But as for integrity, we evaluate the reliability and correctness of data.

Availability: Availability deals with preventing unauthorized withholding of information or resources. In other words, availability guarantees authorized users can access information anytime they want, do so without interference, and receive it in the correct and desirable pattern. The frequent occurrence of popular DoS attacks is mainly attributable to this aspect of information security not being sufficiently addressed.

With the rapid expansion in the theory and practice of information security, the C.I.A. triangle calls for a combination of other parameters.

Authenticity: The quality or state of being genuine or real, instead of a reproduction or fabrication.

Accountability: The defining and enforcement of the responsibilities of the agents (Janczewski and Colarik, 2005).

Non-Repudiation: The property which prevents an individual or entity from denying having performed a particular action related to data or information (Caelli et al., 1991).

In short, the **objective** of information security guarantees that during the procedures of data processing, transmission, or storage, the information is always available whenever it is required (availability), only to those authorized users (confidentiality), and cannot be modified without their authority (integrity). It also means that the user is ensured to use the data in an authenticate representation (Janczewski and Colarik, 2005). There is also a term called computer security, which is a little bit similar to information security. However, we should make explicit the difference between them. The former covers issues only limited to the electronic data processing environment, while the latter deals with more than these issues and includes the whole organization. For example, information security is concerned with the approach paper documents are stored or processed, while computer security is not.

2.2 The Interacting Agents

Generally, the realm of information security involves four groups of agents that interact with each other - hackers, end-users, software vendors, and security specialists. Since most people are quite familiar with end-users and software vendors, we plan to focus on illustrating the other two categories of agents, namely hackers and security specialists.

2.2.1 Hackers

Not all hackers are malicious as most people expect. On the whole, hackers can be divided into two general classes: white hat hackers and black hat hackers (Leeson and Coyne; Schell and Dodge, 2002).

White Hat hackers are also known as the good hackers. Although these hackers break into computer systems without legal rights or privileges, they do not have malign intentions to compromise the systems and voluntarily share security vulnerabilities to help create a good information security environment with those who are in charge of the systems, such as network administrators, CERT/CC, etc. White hat hackers can be further roughly divided into the following three categories (Schell and Dodge, 2002):

- **The Elite** who are the gifted segment, recognized by their peers for their exceptional hacking talent.
- **CyberAngels** who are the so-called "anti-criminal activist" segment of the hacker community patrolling the web to prevent malicious attacks.
- **The White Hat Hacktivists** who strive to promote free speech and international human rights worldwide by constructing websites and posting information on them, using the Internet to discuss issues, forming coalitions, and planning and coordinating activities.

Black Hat hackers are also called the bad hackers. In contrast to white hat hackers, these groups of hackers use exploits to compromise the confidentiality, integrity, or accessibility of the system for a variety of motivational factors such as peer recognition, profits, greed, curiosity, etc., and pose great threats to information security. However, many security experts have proposed that “hackers are not a homogenous group” (Sterling, 1992; Post, 1996; Denning, 1998; Taylor, 1999). And hackers, even black hat hackers, are too broad to be helpful for in-depth researches. Rogers (1999) is among one of the first few security researchers who proposes a new taxonomy for black hat hackers, which categorizes them into seven groups including Tool kit/Newbies (NT), cyberpunks (CP), internals (IT), coders (CD), old guard hackers (OG), professional criminals (PC), and cyber-terrorists (CT). These categories are considered as a continuum from the lowest technical ability (NT) to the highest (OG-CT).

- **Tool kit/Newbies** are novices in hacking and have limited amounts of computer and programming skills. They often rely on published software or exploits conducted by mature hackers to launch the attacks.
- **Cyberpunks** have better computer and programming skills compared with Newbies, and are intentionally engaged in malicious acts, such as defacing web pages, sending junk mails (also known as spamming), credit card theft, and telecommunications fraud.
- **Internals** consist of disgruntled employees or ex-employees who are quite computer literate and may be involved in technology-related jobs before. The most terrible aspect is that they have been assigned part of the job; therefore, they can launch the attacks easily and even without detection.
- **Old Guard Hackers** have high levels of computer and programming skills and seem to be mainly interested in the intellectual endeavor. Although they do not intend to compromise the system, there is an alarming disrespect for personal property from this group (Parker, 1998).
- **Professional Criminals and Cyber-terrorists** are probably the most dangerous groups. They possess advanced computer and programming skills, master the latest technology, are extremely well trained, and often serve as “mercenaries for corporate or political espionage” (Beveren, 2001).

Most of the academic researches have centered on cyber-punks, and little attention has been focused on other classes (Rogers, 1999). Again, it should also be noted that not all hackers are detrimental to the society. Although many black hat hackers exploit security vulnerabilities out of various motivations, we should also look at the other side of the coin. In many cases, the compromise of systems can actually help establish more effective security infrastructure in the future, thus preventing other hackers from launching further attacks. Thus, Schell and Dodge (2002) argue that "hackers represent one way in which we can help avoid the creation of a more centralized, even totalitarian government. This is one scenario that hackers openly entertain".

History of Hacking

After discussing the different classifications of hackers, the history of hacking is introduced next, which implies a constantly changing hacker label (Hannemyr, 1999). The term hacker was coined and presented in the 1960s at the outset of the computer age. Initially, it implied the most capable, smart, competent, and elite enthusiasts mainly in the field of computers and software (Levy, 1984). Since then, hackers have undergone approximately four generations of evolution (Voiskounsky and Smyslova, 2003). The first generation of hackers involves those who actively engaged in developing the earliest software products and techniques of programming. The second generation is involved in developing PCs and popularizing computers. Those who invented popular computer games and brought them to the masses are classified as the third generation. With the development of technology, especially the Internet, the meaning of hacker has changed dramatically. Due to the successive occurrences of information security breaches (Computer Crime & Intellectual Property Section, 2006) and the exaggerated demonization of the media against hackers (Duff and Gardiner, 1996), the term hacker currently carries negative implications of computer criminals and virtual vandals of information assets (Chandler, 1996). Taylor (1999) characterized the fourth generation of hackers as those "who illicitly access others' computers and compromise their systems". In addition, many researchers now hold the viewpoint that "modern hackers are just pirates, money and documentation stealers, and creators of computer viruses" (Taylor, 1999; Sterling, 1992) and "hackers are a national security threat and a threat to our intellectual property" (Halbert, 1997). In conclusion, the term hacker has transformed dramatically from positive images mainly referred to as "white hat" hackers into negative connotations chiefly representing "black hat" hackers.

2.2.2 Security Specialists

In the field of information security, security specialists mainly include CERT® Coordination Center (CERT/CC) (Png, Tang, and Wang, 2006), which is "a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University"[3]. The objective of CERT/CC is to work as a third-party coordinator that conducts extensive researches on information security vulnerabilities, helps develop and establish a sound information security environment, and serves as a bridge between software vendors and end-users. The typical sequence of events concerning CERT/CC can be described as follows: A white hat hacker might first identify a system vulnerability in the software and then report it to CERT/CC. After receiving the report, CERT/CC conducts careful researches to investigate the severity of the vulnerability. If it may pose severe threats, then CERT/CC will notify the concerned software vendors of the vulnerability and provides them with a certain period of time (generally 45 days) to offer patches or workarounds. After the period expires, CERT/CC will issue public advisories, which provides technical information about the vulnerability and patch information that enable users to take preventive actions and protect their systems against potential malicious attacks.

2.2.3 Overall Sequence of Events

The overall sequence of events involving the four groups of agents can be best illustrated by Figure 2.1 (Png, Tang, and Wang, 2006).

[3] Interested readers can refer to www.cert.org for detailed information.

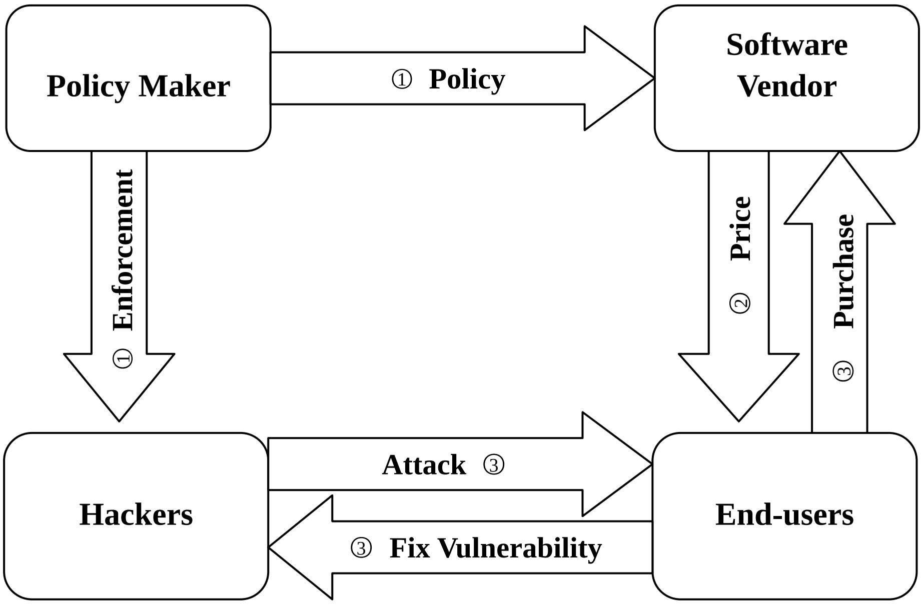

Figure 2.1: Sequence of Events

2.3 Barriers to Sound Information Security - Insufficient Incentives

A review of the literature (e.g., Anderson, 2001; Varian, 2000; Kunreuther and Heal, 2003; Camp and Wolfram, 2000, etc.) indicates that the major culprit to information insecurity results from **insufficient incentives**. Anderson (2001) is among the first few security experts who put forward the innovative idea - “information insecurity is at least as much due to perverse incentives”. At present, after an extensive literature review, we classify the main reason - insufficient incentives - into four main categories that pose as barriers to sound information security.

2.3.1 Negative Network Externalities

Negative externalities[4] occur when one party directly imposes a cost to others without any compensation. Consider, for example, the following scenario: In a computer network composed of 100 users who can choose whether or not to invest in information security, if others are active to invest in security, then you may also benefit the enhanced security generated from positive externalities; therefore, you

[4] A good introduction to network externalities is presented by Shapiro and Varian (1999).

might prefer to be a “free rider”, and choose not to invest in security and save money. On the other hand, if others are reluctant to invest in security, then the incentive for you to do so is greatly diminished, since the computer network often assumes a “friendly” internal environment and only protects external attacks instead of viruses coming from the internal network, and a smart hacker can attack and compromise all the other computers via some unprotected ones. “The overall security of a system is only as strong as its weakest link” (CSTB, 2002). It seems that, in a computer network now prevalent in the real world, the issue of information insecurity cannot be eliminated thoroughly no matter whether or not users invest in security. Kunreuther and Heal (2003) first proposed the issue of interdependent security (IDS), and developed an interdependent security model to address the incentives of investing in security. The central theme in their paper is that when all the agents are identical, two Nash equilibria exist - either everyone invests in information security or no one bothers to do so, and under such circumstance, only stipulating that everyone should invest in security can enhance social welfare, which can resolve the above dilemma. Kunreuther et al. (2003) further points out that when there are a large number of identical agents ($n \to \infty$) and none of the others has invested in security, then investing in computer security for the remaining one agent is *by no means* a dominant strategy in Nash equilibrium provided that the cost of protection is positive.

Another potential harm caused by negative externalities in information security is rooted in the large installed base of the products involved. Just as a coin has two sides, in spite of great benefits of enhanced compatibility and interoperability, a large installed base can also attract a considerable amount of malicious attacks, thus rendering the consumers more vulnerable to security breaches both within and outside the organization (Rohlfs, 1974). Malicious black hat hackers prefer to attack systems with a large installed base due to higher market share and thus greater economic payoffs to exploit potential vulnerabilities. Accordingly, by participating in a larger network, an individual or firm encounters higher security risk despite enhanced compatibility and interoperability. That is the reason why most hackers have an unrelenting enthusiasm to launch attacks towards Windows-equipped machines (Honeynet Project, 2004; Symantec, 2004).

To address the issue of negative externalities, governments can try to force the firms involved to internalize the externalities in the following ways:

(a) Requiring firms to buy security insurance in case of possible security breaches, which is also related to an attractive research field - cyber-insurance;

(b) Stipulating that software vendors should be responsible for the low-security products, and computer owners and network operators be held accountable for the financial losses caused by the security breaches via their computers to third parties;

(c) Providing governmental financial supports such as public subsidies to those who invest in information security to further motivate them to contribute to a sound security environment.

However, not all the above approaches are feasible and efficient. For example, the second way is too expensive to enforce because of high transaction costs to determine the liability party as well as the culprit of the losses - the identification of the cause might sometimes take several months or even years (Kunreuther and Heal, 2003). But, anyway, the above points establish a solid foundation for further improvements, and their efficacy needs to be empirically tested in the real world.

2.3.2 Liability Assignment

The second cause of insufficient incentives resides in deficient or ill-defined liability assignment. Consider, for instance, the following scenario: A black hat hacker discovers a security vulnerability at site A to attack via network operated by B through Internet Service Provider (ISP) C, which compromises the information in the D’s computer. Then who should be responsible for the security breach? No one is willing to hold accountable for it. This is called inadequate “liability assignment” (Varian, 2000). Similar situations are ubiquitous in the real world. In the field of information security, the liability is also so diffuse, thus rendering the large quantity of information security breaches. For example, since software vendors are not held accountable for the low quality and security of the products, they tend to shift the burden to their consumers without any loss and do not bother to improve security. Another example is related to some high profile websites that have been attacked by malicious hackers via unprotected and compromised computers. Although the system operators or computer owners do not intend to participate in the attacks, they indirectly help the hackers to commit criminal actions and even do not bear the costs of the attacks. The two examples illustrate the same idea: the parties involved do not have sufficient incentives to protect the information security due to ill-defined liability assignment.

To address the issue, Varian (2000) argues that one of the fundamental principles of the economic analysis of liability is that it should be assigned to the party that can perform the task of managing information security in the most efficient manner. A more concrete approach is to assign liability in two ways: (a) System operators and computer owners should be liable for the financial losses caused by malicious attacks via their computers to third parties such as denial-of-service to high profile websites, and (b) Software vendors should be held responsible for their low-security products. An alternative method is to “allocate a set of vulnerability credits” to every individual machine and create tradable permits just like the way used in pollution (Camp and Wolfram, 2000). Other potential solutions for addressing liability assignment include establishing insurance markets to handle security risks and requiring firms to buy the cyber-insurance (Blakely, 2002). However, some controversies exist concerning who should be liable for security breaches (Fisk, 2002; Camp and Wolfram, 2000). To make matters worse, legal systems do not fully address the liability party in terms of computer security either. Up till now, U.S. case laws have not yet explicitly clarified who should shoulder the responsibility for financial losses when IT security is compromised caused by breaches to the damaged party (Ashish, Jeffrey et al., 2003).

Of course, someone who has learned "*The Coase Theorem*[5]" might claim that in the absence of transaction costs, an efficient outcome exists no matter how allocations of properties are assigned. However, the most important premise - no transaction cost - is almost impossible to fulfill in the real world. In dealing with security incidents, determining the liability parties involved generally entails substantial time and efforts - high transaction costs. Therefore, when this precondition is not satisfied, the Coase Theorem fails to provide any promising direction for governmental policies in this setting.

2.3.3 No Accurate Measures of Information Security

Another reason why there are insufficient incentives in protecting information security results from the dearth of accurate measures of good information security. Today, the information security market is actually a "market for lemons[6]" in the sense that evaluations of product security are blurred by consumers' inability to distinguish secure products from insecure ones, thus leading to little incentives to increase the security of the products (Anderson, 2001; Blakley, 2002). The situation is further aggravated by software vendors' strong motivations to incorporate many attractive features but often possibly including some new vulnerabilities (European Union, 2001).

To address the issue, a large quantity of metrics have been proposed to measure information security, such as Annual Loss Expected (ALE), Security Savings (S) and Benefit (B) (Hoo, 2000), Investment Return: Return on Investment (ROI) (Blakley, 2001) and Internal Rate of Return (IRR) (Gordon and Loeb, 2002), etc. However, all of the above measures have some limitations, which will be discussed in detail in the next chapter. A relatively innovative measure is presented by Schechter (2004), who uses the market price to identify a new vulnerability (MPV) to measure security strength. Although this method can be used to establish a vulnerability market and

[5] Interested readers can refer to Coase (1960) for a detailed explanation of the Coase Theorem, and can also read Frank (1999) for a brief introduction.

[6] For a detailed idea of "the market for lemons", readers can refer to Akerlof (1970).

improve information security, Ozment (2004) argues that Schechter fails to consider some fundamental problems such as expense, reputation, and copyright infringement, and "the expense of implementing the vulnerability market is not trivial".

2.3.4 Other Barriers to Information Security

In addition to the above three barriers, other obstacles to information security should by no means be neglected.

First, a couple of empirical studies (Ackerman, Cranor, and Reagle, 1999; Westin, 1991) have reported that consumers place high values on privacy. However, some recent surveys and experiments (Chellappa and Sin, 2005; Hann, Hui, Lee, and Png, 2002) have pointed out the obvious "dichotomy between privacy attitudes and actual behaviors" (Acquisti and Grossklags, 2005) - many consumers are willing to trade off privacy for small rewards such as $2 or a free hamburger, which poses a great threat to information security, since once hackers obtain consumers' personal information, it is quite easy for them to launch attacks such as identity theft.

Second, considering that the probability of security breaches is relatively low, consumers might find that security safeguards will bring about functional problems such as declining convenience, slow speed, etc. Besides, many consumers might prefer to purchase the products focusing on attractive features instead of enhanced security, that is, to trade off security for functionality.

Third, many firms just do not report information security breaches, since they fear it will endanger their reputation or publicity. Actually, concealing such facts does nothing but hampers the establishment of sound information security. It is no wonder for Pfleeger (1997) to argue that "the estimated security breaches might be the tip of a very large iceberg".

Finally, although home security benefits exceptionally from regression models, information security cannot use similar models to measure security risks. The underlying reasons are as follows: (a) Information systems are much more “complex and heterogeneous than homes”, and (b) The relationships between independent variables and dependent variables are dynamic rather than static (Schechter, 2004). Therefore, although both information security and home security belong to the category of security, the former cannot use traditional regression models to measure security risk unless we can successfully isolate the dynamic factors from static ones.

In conclusion, the following paragraph is presented to wrap up this section of barriers to sound information security. Anderson (2001) concludes “the real driving forces behind the security system design usually have nothing to do with such altruistic goals. They are much more likely to be the desire to grab a monopoly, to charge different prices to different users for essentially the same service, and to dump risk”. In addition, economics often serves as an efficient as well as effective weapon to properly align incentives. Therefore, we have the firm conviction that economic approaches should be promoted and employed to address the issue of information security, which will be discussed in detail in the following chapter.

Chapter 3 Traditional Measures to Address Information Security

In Chapter 1.1, we have illustrated in detail the motivations to implement information security. In addition, Chapter 2.3 presents the challenges to maintaining sound information security atmosphere. Therefore, it is urgent for us to take some preventive measures to address information security. An extensive literature review points out three main directions of research endeavor, namely, technological approaches, behavioral aspects, and economic approaches to information security. Since this paper mainly deals with economic aspects of information security, technological approaches to address security are introduced in brief, just as a refresher introduction.

3.1 Technological Approaches

At first, information security was considered as a pure technological issue which simply called for technical defense. Under such circumstances, a large branch of researches and a large number of research papers have centered on the design and implementation of security technology. Technical solutions, if properly implemented, are able to maintain the confidentiality, integrity, and availability of the information assets. Technical defense includes firewalls, intrusion detection systems (IDS), dial-up protection, scanning and analysis tools, content filters, trap and trace, cryptography and encryption-based solutions, access control devices, etc (Whitman, 2003; Dhillon, 2006). Among these techniques, encryption-based solutions, access control devices, IDS and firewalls aimed at safeguarding information security attract the largest amount of attention from security experts (e.g., Wiseman, 1986; Simmons, 1994; Muralidhar, Batra, and Kirs, 1995; Denning and Branstad, 1996; Schneier, 1996; Pfleeger, 1997; Larsen, 1999). Although technological approaches were once “hailed as the magic elixir that will make cyberspace safe for commerce” (Varian, 2000), Anderson (1993) argues that most of the ATM frauds involve human errors, and they are caused by implementation errors or management failures rather than deficiencies in cryptosystem technologies. In other words, simply relying on technical defense alone, it is still hard to properly address information security due to insufficient incentives, and we should also employ the powerful economic tools - microeconomics - to better align economic incentives in order to establish sound information security.

3.2 Behavioral Aspects

In addition to technological approaches discussed above to addressing information security, researches on behavioral aspects to diminish security breaches have been developing rapidly (e.g., Straub, 1990; Niederman, Brancheau, and Wetherbe, 1991; Loch, Carr, and Warkentin, 1992; Straub and Welke, 1998; August and Tunca, 2005).

A promising and significant research direction involves the exploration of motivational factors relating to hackers. As early as in 1994, Schifreen (1994) proposed five motivational factors that pushed hackers to conduct hacking activities, which included opportunity, revenge, greed, challenge, and boredom. Taylor (1999) is probably the earliest comprehensive publication that investigates hackers' motivations, which presents that hackers' motivations are categorized into six main groups: feelings of addiction, urge of curiosity, boredom with the educational system, enjoyment of feelings of power, peer recognition, and political acts. While acknowledging Taylor (1999)'s contributions, Turgeman-Goldschmidt (2005) challenge that none of these motivations is closely related to the hackers' mental product. Thus, he argues that hackers' accounts instead of their motivations should be examined to further extend the understanding of hacker community. The hackers' accounts reported by the interviewees in his study are presented in the following descending order of frequency: 1) Fun, thrill, and excitement, 2) Curiosity for its own sake - a need to know, 3) Computer virtuosity, 4) Economic accounts - ideological opposition, lack of money, monetary rewards, 5) Deterrent factor, 6) Lack of malicious or harmful intentions, 7) Intangible offenses, 8) Nosy curiosity and voyeurism, 9) Revenge, and 10) Ease of execution. Furthermore, the author indicates that fun, thrill, and excitement is fundamental to all the other accounts due to the fact that all of them rely on it. For example, the second point - curiosity - can be interpreted as the fun of discovering, knowing, and exploring. The author's use of hackers' accounts is a creative extension to Taylor (1999)'s work because it enables researchers to comprehend how people perceive themselves within their own cultural context and serves as an interpretive structuring of reality of hacker community (Turgeman-Goldschmidt, 2005). A conceptual theoretical model is developed by Beveren (2001) to describe the development of hackers and their motivations. Its selling point is to use the flow (Csikszentmihalyi, 1977, 1990, 1997) construct to present important variables that network operators and website designers can employ to deter and prevent malicious attacks in daily operations if the hypotheses proposed are supported by empirical studies.

In order to gain a deeper understanding of the social foundation that enables hackers to evolve into a unique social group, Jordan and Taylor (1998) explore the nature of the hacking community by focusing on two aspects: internal factors and external factors. The internal factors involve six elements: technology, secrecy, anonymity, boundary fluidity, male dominance, and motivations. The six components mainly interact with each other among hackers, and equip them with a common language and a variety of resources hackers can utilize to communicate, recognize, and negotiate with each other within the border of the hacking community. The authors then explore the external factors by emphasizing defining the boundary between their community and the computer security industry. The boundary represents an ethical interpretation of hacking activity in the sense that distinguishing the activities and membership of the two entities poses a difficult problem to researchers (Jordan and Taylor, 1998). Finally, the authors reject the partial perspective of the demonization and pathologization of hackers as isolated and mentally unstable, and suggest that "hacking cannot be clearly grasped unless fears are put aside to try and understand the community of hackers, the digital underground" (Jordan and Taylor, 1998).

Most of the previous studies are based on anecdotal and self-reported evidences. To address this problem, Voiskounsky and Smyslova (2003) present an empirical analysis of hackers' motivations. The underlying model is flow theory/paradigm originated by Csikszentmihalyi (1977), which means that "an action follows the previous action, and the process is in a way unconscious; flow is accompanied by positive emotions and is self-rewarding". The most important component of flow theory is the precise matching of people's skills and task challenges (Voiskounsky and Smyslova, 2003). The empirical results demonstrate that the claim that intrinsic motivation (flow) motivates hackers to engage in hacking activities is supported as expected. Besides, the least and the most competent hackers experience flow, while the moderately competent hackers undergo "flow crisis", which can be eliminated by properly aligning skills with task challenges - the process of flow renovation, thus starting to experience flow anew. Their results are considered as innovative and revealing in the sense that it rejects the generally accepted hypothesis that the more qualified and competent the hackers are, the more flow they experience than their less qualified counterparts (Novak and Hoffman, 1997).

Mulhall (1997) argues that although there are large quantities of articles involving the exploration of hackers' motivations, the stream of research is, in a sense, static, which means it is not utilized to examine how to deter hackers from committing hacking activities. Mulhall (1997) advocates that legal remedies can serve as a deterrent factor to hackers and physical or logical barriers to hackers coupled with imprisonment punishment can work well. The second effective deterrence is hackers' fear of being caught. Hackers are afraid of being apprehended, which can have a substantially negative impact against such aspects as future career prospects, parental action, and the confiscation of the equipment. Finally, the author suggests that good access control systems together with detection and legal punishment are conducive to deterring hackers. Other researchers also examine the deterrent factor in the field of information security, which involves two ingredients: the probability of being apprehended and the severity of the punishment. Ben-Yehuda (1986) indicates that only if both ingredients are at a high level are hackers discouraged from committing hacking activities. However, in the status quo of computer-related offenses, both components are at a low level (Ball, 1985; Bloom-Becker, 1986; Hollinger, 1991; Michalowski and Pfuhl, 1991).

Lakhani and Wolf (2005), in an attempt to understand the relative success of Free/Open Source Software (F/OSS) campaign, are interested in the investigation of the factors that motivate F/OSS developers to contribute their time and efforts to create free software products. They suggest that intrinsic motivation including enjoyment-based and obligation/community-based is the strongest and most perceivable impetus for project participation rather than external factors in the form of extrinsic benefits such as better jobs and career advancement proposed by previous academic researches (Frey, 1997; Lerner and Tirole, 2002). Their final results are summarized as follows: efforts in F/OSS projects are original exercise, bringing about useful output, and are motivated most by the creativity an individual feels in it. Of course, the authors also argue that both extrinsic and intrinsic motivations interact with each other - neither one is able to dominate or cancel the other. F/OSS developers are motivated by a blend of intrinsic and extrinsic motivations with individual creativity as the most significant driver of project participation. The paper complements the existing body of research by investigating the motivational factors of hackers' from the perspective of F/OSS and advancing our understanding of the underlying motivations in the F/OSS community.

Other research directions also abound in the field of behavior aspects. Straub (1990) places emphasis on the design of deterrent, detection, and preventive measures for institutions to control information security risks, which helps reduce the probability of security breaches. Boss (2005) investigates information security from both a behavioral and control perspective, and establishes a theoretical model that incorporates the three basic elements of control theory - measurement, evaluation, and reward - to examine the efficacy of behavioral controls on the overall security efforts within the organizations. Schneier (2005), a pioneering security expert, concludes that modern hacking has been transforming from a hobbyist activity into a criminal one ranging from pursuing substantial economic profits to seeking political revenges such as cyber-terrorism, which makes them more dangerous and devastating. Furthermore, Schechter and Smith (2003) identify and introduce a new type of worm that separates the endeavor of creating back-door vulnerabilities from the activity of installing and exploiting them on the vulnerable systems. The outcome is minimized risk[7] and increased incentives to worm's authors, which makes worms more lucrative to write. The authors suggest being alert and careful in using existing security actions to safeguard organizations against the use of "access-for-sale" worms.

Although technology-based approaches discussed in Chapter 3.1 do help to resolve the issue of information security to some extent, even the perfect technology cannot perform successfully unless people involved install, configure, and manage these technologies in a correct manner. This is where behavioral methods can kick in and play a role. Sometimes, putting ourselves in hackers' shoes, thinking like a hacker, and investigating hackers' motivations can place us in a more favorable position to safeguard against security breaches.

3.3 Economic Approaches to Information Security

Compared with technological and behavioral approaches discussed in Chapter 3.1 and 3.2, economic approaches have only recently been applied to the field of information security (Gordon and Loeb, 2002) and researches focusing on the economic aspects of information security are relatively sparse (Schechter, 2004). However, with the successful promotion of WEIS[8], this field is developing at an alarming rate and attracting an increasing amount of attention from both economists and security experts. The seminal paper (Anderson, 2001) points out the main culprit of the increasing number of information security breaches - insufficient incentives, establishes the

[7] The risk to the worm's author is minimized in the sense that he/she does not need to communicate with the vulnerable systems, reducing the risk of being detected.

[8] WEIS (the Workshop on the Economics of Information Security) is an annual seminar event first held in 2002 to cultivate and intrigue researches in the field of information security.

importance of economic approaches to information security, and serves as a milestone for later researches in this field. On the whole, we further classify economic approaches to information security into five main streams of research directions, that is, strategic interactions between hackers and end-users, software vulnerability disclosure and patch policies, optimal investment in information security, liability assignment and cyberinsurance, and evaluations of information security technologies.

3.3.1 Strategic Interactions between Hackers and End-users

Information security is an endeavor involving four groups of agents - end-users, black hat hackers, software vendors, and security specialists such as CERT/CC (Png, Tang, and Wang, 2006). There is a large stream of researches focusing on the respective groups of agents.

End-users: Kunreuther and Heal (2003) study the incentives of end-users and derive the useful result that the incentives of users to invest in information security decrease as the number of unprotected agents increases assuming that all agents are identical. August and Tunca (2005) examine the users' incentives to patch security vulnerabilities, and demonstrate that in some situations, mandatory patching is sub-optimal.

Black hat hackers: Beveren (2001) develops a conceptual model to portray the development of hackers and their motivations. He uses the flow construct that serves as moderators to model the evolution of a hacker's experience. Jordan and Taylor (1998) argue that potential malicious motivations such as greed, power, authority, and revenge are replacing such benign motivations as curiosity.

Software vendors and security specialists: In the field of information security, we mainly discuss the interactions between software vendors and security specialists such as CERT/CC. Since the policies CERT/CC enacts will have a substantial effect on vendors' incentives to invest in information security such as producing products of higher security or providing patches more quickly, etc., this research field has drawn a lot of attention among economists and security experts. The typical research papers include Beattie, Arnold, Cowan, Wagle, and Wright (2002), Arora and Telang (2005), Rescorla (2004), Arora, Krishnan, Telang, and Yang (2005), Browne, McHugh, Arbaugh, and Fithen (2000), Nizovtsev and Thursby (2005), Choi, Fershtman, and Gandal (2005), Anderson and Schneier (2005), Arora, Forman, Nandkumar, and Telang (2006), Png, Tang, and Wang (2006), to name just a few.

3.3.2 Software Vulnerability Disclosure and Patch Policies

One of the most heated and intense debates in information security deals with software vulnerability disclosure and patch policies. The main issues include such open research questions as: (a) The effect of vulnerability disclosure policy on vendors' behaviors, (b) Optimal patch time, and (c) Relationships between the number of security breaches and time.

- **The Effect of Vulnerability Disclosure Policy on Vendors' Behaviors**

Although there is a consensus about the goal of vulnerability disclosure, opinions concerning whether full or partial disclosure policy should be established differ dramatically, which mainly fall into three categories. Some people argue that the details about the information of a vulnerability, including the tools that exploit it, should be instantly disclosed to the public, while the other extreme is called partial disclosure that advocate waiting and disclosing the flaws only after vendors have provided the appropriate patches. Besides, some hybrid disclosures combining the above two also exist in the real world. Full disclosure provides strong incentives to the vendors to release patches as early as possible (Pond, 2000); however, this practice leaves users in a precarious state if there are no appropriate patches to fix the vulnerabilities. Therefore, it might be socially undesirable and does not necessarily improve overall social security (Elias, 2001; Farrow, 2000).

Arora, Telang, and Xu (2004a) take into consideration three groups of parties - software vendors, end-users, and social planners, and develop a theoretical model to investigate the effect of early disclosure on vendors' behaviors and the resulting welfare implications. The interesting result indicates that early disclosure of vulnerabilities will lead to vendors patching flaws faster, although it might be socially sub-optimal. Arora, Telang, and Xu (2004b) argue that neither full nor partial disclosure is optimal in certain specific situations. Wattal and Telang (2004) holds the viewpoint that full and immediate disclosure provides impetus for vendors to improve the quality and security of their products. Arora and Telang (2005) establish a theoretical framework to identify the major ingredients that determine the appropriate method of dealing with vulnerability disclosure. They assert that faster disclosure motivates vendors to patch more rapidly, but a remarkable portion of users still do not fix the patches appropriately. Rescorla (2004) argues that a large quantity of resources expended on identifying and patching security breaches does not lead to a remarkable quality enhancement of software products. Therefore, the claim that vulnerability disclosure can result in enhanced product quality is untenable. Only if vulnerability disclosure is significantly correlated, then it is advisable to disclose software vulnerabilities; otherwise, it will cause substantial losses to the victims. The result is quite novel and discouraging to vulnerability disclosure, but whether the claim is valid or not requires further empirical analysis using more recent data sources and more advanced economic models in further researches.

- **Optimal Patch Time**

Another important research question in the case of information security is to derive the optimal patch time that minimizes the losses. Patched too soon or too frequently, it will incur great operational costs, which is sometimes unaffordable. Besides, the patches may not be tested thoroughly, which might have some other potential vulnerabilities. On the other hand, if patches are released too late or less frequently, the systems are left in a precarious state subject to vulnerability exploits by the hackers. Therefore, it involves a tradeoff between the above two choices and that is the reason why this field is attracting an increasing number of attention from security experts and economists.

Beattie, Arnold, Cowan, Wagle, and Wright (2002) propose a theoretical model to investigate the factors determining when it is optimal to apply security patches. In addition, they also use empirical data to provide the model with more practical value.

They argue that the optimal time to apply security patches is 10 and 30 days after the release of the patches, which can serve as best practices adopted by security practitioners when they need to apply security patches. Cavusoglu, Cavusoglu, and Zhang (2006) construct a game theoretical model to determine the optimal frequency of updating security patches, which resolves the tradeoff between high operational costs and security risks subject to hackers' exploiting vulnerabilities. They analyze two settings, namely centralized and decentralized systems, respectively, and, in the decentralized setting, successfully resolve the problem of how to coordinate the patch release policy adopted by software vendors and the patch update policy taken by the companies that use such mechanisms as cost sharing or legal liability, which means that the optimal patch management entails appropriate synchronization of patch release and update practices. However, several limitations compromise the applicability of the results derived. The authors assume that one computer has exactly one vulnerable software subject to malicious exploits. But, it is not necessarily the case in the practical situations. Furthermore, the severity of different vulnerabilities is set constant (exogenous), because it is generally hard to distinguish severe security flaws from non-severe ones (Donner, 2003). The results might be more valid and convincing if these problems can be addressed more appropriately.

- **Relationships between the Number of Security Breaches and Time**

Common sense tells us that the number of security breaches will increase with the time since the start of the exploit cycle. However, the accurate relationships such as linearity or non-linearity are, to a large extent, non-trivial and untouched. One of the pioneering empirical researches is Browne, McHugh, Arbaugh, and Fithen (2000)'s paper that conducts an empirical study investigating the relationships between the number of security breaches and time since hackers first exploited the vulnerabilities. They find that the number of security breaches increases in proportion to the square root of the time, which can be modeled with the following formula: $C = \beta_0 + \beta_1 \times \sqrt{T}$, where C is the number of security incidents and T is the time. To the best of our knowledge, the paper is the first scholarly endeavor that addresses this relationship, and the model can be used to predict the rate of incidents' growth as well as to enable organizations to proactively rather than reactively allocate appropriate resources to deal with security breaches.

3.3.3 Optimal Investment in Information Security

With the tendency of organizations' increasing dependence on information systems and billions of dollars expended on information security, economics of information security investment has drawn more and more attention and has become an important branch of economics of information security with significant implications for organizational practices. This direction mainly involves researches that identify optimal security investment levels under different circumstances. The seminal research can be ascribed to the study of Gordon and Loeb (2002), which innovatively presents a simple and relatively general economic model that determines the optimal amount of a company's investment to safeguard corporate information assets against security breaches in a single-period setting. They examine two broad classes of security breach probability functions and derive a quite interesting result that for those two classes of functions, the optimal amount of security investment should by no means exceed $1/e \approx 37\%$ of the expected losses caused by security breaches. Nevertheless, Willemson (2006) successfully finds the counterexamples to the above result and claims that whether the universal upper limit exists is open to question, since the real situations might fall beyond the two general classes of functions. Further directions for improvement to Willemson (2006) include investigating other aspects of information security investments such as enhanced government enforcement to increase the attacks' costs in addition to simply considering users' efforts to decrease the probability of security breaches. Huang, Hu, and Behara (2006) propose an economic model that investigates simultaneous attacks from multiple external agents with distinct characteristics, and derive the optimal investment level in this context. It also distinguishes two types of security attacks: distributed and targeted attacks, which are often neglected by just focusing on the total attacks. Therefore, this paper fills the void by providing significant implications concerning these two types of attacks to organizations. The main results are as follows: (a) Since a company encounters both distributed and targeted attacks, when the budget is relatively small, it is advisable to allocate the money to distributed attacks, because distributed attacks can be safeguarded against more efficiently and with relatively smaller investments, (b) When losses from targeted attacks are very substantial, the company had better invest all its money to prevent targeted attacks even if the budget is quite limited, and (c) The percentage of the investment in safeguarding targeted attacks increases when the budget augments. However, this paper is by no means free from limitations. It only considers the company as a risk-neutral agent like that in Gordon and Loeb's model (2002), while most of the firms are risk-averse in the real situation. Besides, the paper fails to investigate the interdependencies of the above two types of attacks, and just examine them independently.

Since the investment in information security always needs to compete for resources with other business opportunities, the chief information security officer (CISO) is required to provide a concrete and convincing analysis of the effect of investments in information security on the organizations concerned in order to justify the need to protect it. The prerequisite of this demanding project is to accurately measure security risks. In the risk management literature, on the whole, three streams of research have evolved to measure security risks: (a) Annual Loss Expected (ALE), (b) Security savings (S) and Benefit (B), and (c) Investment Return: ROI and IRR. Table 3.1 summarizes the approaches to employ these three metrics. However, each of these metrics has certain limitations, which compromises its applicability into real problems.

To accurately measure security attacks, Schechter (2004) proposes an original metric - security strength, which uses the market price to find a new vulnerability (MPV) as a measure of security strength. The novel metric MPV can also be used to differentiate secure products from insecure ones by establishing an upper bound on the MPV of the competing products below that of the lower bound of its own products' MPV.

However, although this approach has served as a milestone for future researches, Schechter's vulnerability market (VM) encounters several challenges, such as the problem of expense, reputation, copyright infringement, etc. Ozment (2004) makes a preliminary effort to identify fields where auction theory can play an active role to improve the efficiency and efficacy of the VM proposed by Schechter. However, it calls for radical changes to the management environment of organizations to implement such a bug auction.

Specific Metric	**Abbreviation**	**Approach to Calculate**
Annual Loss Expected	ALE	Expected rate of loss * Value of loss
Savings	S	$\text{ALE}_{\text{baseline}} - \text{ALE}_{\text{with new safeguards}}$
Benefit	B	S + (Profit from new ventures)
Return On Investment	ROI	$\frac{B}{\mathit{Cost}\text{ of safeguards}}$
Internal Rate of Return	IRR	$C_0 = \sum_{t=1}^{n} \frac{B_t - C_t}{(1 + IRR)^t}$

Table 3.1 Common Metrics to Measure Security Risks

3.3.4 Liability Assignment and Cyberinsurance

Although organizations are generally increasing the investment in information security (Mears, 2004), the current security environment has left most of them in a precarious state (Gordon, Loeb, and Lucyshyn, 2005). Anderson (2001) asserts that information security calls for more economic approaches than simply technological methods, and that sufficient economic incentives should be established first as a solid foundation in order to implement technical defenses more appropriately (Anderson, 1993). Varian (2000) further identifies misplaced liability assignment as the main cause of information insecurity. He advocates that liability should be assigned to the party that can manage and prevent security risks in the most efficient manner. In the real world, Varian argues that network operators and computer owners should be responsible for the financial losses caused by security breaches via their computers to third parties, and software vendors are to be held accountable for vulnerabilities in their products. Another innovative idea in his paper is that the parties that have the liability for security breaches can and should outsource the risks and buy cyberinsurance. In this way, firms are safeguarded against potential losses of damaging security risks or indemnification parties. Following Varian (2000)'s lead, many economists are conducting related researches that apply insurance to information security - so called "cyberinsurance[9]". Majuca, Yurcik, and Kesan (2006) write a good paper by tracing the evolution of cyberinsurance from traditional insurance policies to current cyberinsurance products, and point out that the status quo of information security environment calls for an increasing demand for cyberinsurance, which can better address security risks. Kesan, Majuca, and Yurcik (2005) employ a simple model demonstrating that cyberinsurance leads to higher security investment, facilitates criteria for best practices, and brings about higher social welfare. Bohme (2005) identifies the correlation in cyber risks, especially prevalent in the current information age, as the major barrier to cyberinsurance. He constructs an indemnity insurance model to claim different premiums for different users, which resolves the correlation problem. However, the model also suffers from several limitations of simplicity and overly strict assumptions in terms of the demand side. As a further endeavor, Bohme and Kataria (2006) find that not all cyber-risk classes have similar correlation attributes, and then manage to introduce a novel classification of cyber-risk classes using a two-tier approach, namely, within-firm tier and global tier, respectively. Furthermore, Baer (2003) summarizes the major impediments that currently limit the scope and effectiveness of cyberinsurance: lack of agreement on basic policy definitions and language, lack of underwriting experience, lack of adequate reinsurance, and policy exclusions.

3.3.5 Evaluations of Information Security Technologies

In this section, we mainly review the current status of honeypots (also called honeynets or honeytokens), which are information system resources employed to be

[9] Cyberinsurance is aimed at reducing cyber risks by providing additional insurance coverage to the realm of information security. Interested readers may refer to Kesan et al. (2005), Amanda (2000), Bohme (2005), etc.

attacked and penetrated to capture activities on them so as to keep track of any misuse and to decrease the risks imposed by the honeypots to other systems (Spitzner, 2003; Honeynet Project, 2001). With the increasing popularity of honeypots in the field of information security, a large stream of researches has been focused on this emerging area, producing a lot of valuable research papers. Dornseif and May (2004) summarize the benefits and costs of implementing honeynets, which is helpful to the understanding of the economic aspects of honeynet deployment. The benefits of employing honeynets include potential information gathered concerning hackers' attacking patterns and potential enhanced security by using honeynets as a decoy and by using aggressive honeynets for redirection. On the other hand, costs of implementing honeynets should also be considered thoroughly, such as costs of deploying, costs of operation, and costs of increased risks to the user's own network (Dornseif and May, 2004). Dacier, Pouget, and Debar (2004) first conduct an experiment with several honeypots implemented for four months and derive many important results: (a) The regularity represented by the data demonstrates the value of using honeypots to track attack processes, and (b) Honeypots should be placed in different locations to eliminate the bias of particular places and produce a relatively general conclusion concerning attacks. Pouget and Dacier (2004) further conduct the honeypot research by devising a simple clustering approach to obtain more in-depth as well as useful information on tracked attacks. They use the algorithms of association rules in Data Mining and phrases distance to identify the root causes of observed attacks, which is very helpful for a deeper understanding of attacks. Their paper applies algorithms in computer science to the economics of information security, which complements the existing body of research in this area. However, the clusters derived are still open for further refinement. In their third academic endeavor, Pouget, Dacier, and Pham (2004) set up a honeypot environment deployed for as long as 18 months and derive useful data to better understand the attack patterns. The results in this paper confirm the findings in their previous researches, which indicate the value of using honeypots to track attack processes. The limitation of their paper might be the relatively concentrated places mainly in Europe where honeypots are deployed.

That is to say, a larger number of honeypots deployed in various places may make the results more convincing and reliable. On the whole, the above three papers pave the way for deploying honeypots to obtain data that can be used to establish empirical models of the attack patterns in the real world.

After a relatively complete literature review of economic approaches to information security, we identify two possible research directions that are worth delving into: (a) Cyberinsurance, and (b) Empirical studies that incorporate government enforcement into the general framework. Cyberinsurance brings about higher security investment, facilitates criteria for best practices, and leads to enhanced social welfare. In addition, cyberinsurance is still rather nascent as an industry and is rapidly expanding in terms of the market share (Peter, 2002). Therefore, it is worthwhile and promising to employ cyberinsurance as a powerful weapon to better address information security issues. A review of the existing literature also reveals that compared with researches on economic modeling, empirical analyses in information security are relatively sparse in quantities due to insufficient and relatively stale data for the variables in the model. Besides, almost no papers described above explicitly take into consideration the effect of government enforcement on hackers' behaviors. Even if some research papers occasionally touch government enforcement, they fail to fully investigate it or subject it to empirical testing. To fill this void, we plan to conduct an empirical study to investigate the effect of government enforcement against hackers' behaviors using real-world data collected from diverse sources. We hope this study can shed light on the impact of cyber-law and cyber-regulation that can effectively and efficiently deter hackers from committing cyber-crimes. The first possible research direction - cyberinsurance - is left as future research work, and this paper centers on the second direction - empirical studies involving government enforcement in the general model. Since event study methodology is employed to investigate the impact of government enforcement, it is necessary to present a brief literature review of event study analysis in the next chapter before discussing its methodology and data source.

Chapter 4 The Effect of Government Enforcement against Hackers' Behaviors

Information security is an issue of important concern to organizations as well as governments, and many researchers have been engaging in this dynamic and promising field. However, while prior researches provide important insights into the behaviors of various parties in the field of information security, nearly none of them directly investigates the effect of government enforcement. The objective of this paper is to fill this gap by focusing on one factor that has been, to the best of our knowledge, untouched yet in former researches and shedding light on the following research question: "What is the impact of government enforcement against hackers' behaviors?". The intuition behind the question is that after the government decides to convict or sentence a hacker and the announcement is released to the public by the media, it will have a deterrent effect on hackers' behaviors characterized by reducing the number of security breaches launched by other hackers in that country.

4.1 Literature Review of Event Study Methodology

In order to measure the effect of government enforcement against hackers' behaviors, event study methodology is adopted. Our methodology follows basically from prior event study analysis (Jarrell et al, 1985; Hendricks et al, 1996; Mackinlay, 1997, etc.). Event study methodology investigates the magnitude of the effect that a specific event has on the market value and profitability of firms associated with this event, that is, whether there is any effect of "abnormal" stock prices related to certain unanticipated event (Agrawal and Kamakura, 1995). The intuition and implicit assumption in this methodology is that security prices respond rapidly and correctly to the infusion of new information and current security prices can reflect all the available information; therefore, any change in the stock prices is a good indicator of the impact of a specific event - the so-called efficient market hypothesis (EMH, please refer to Fama et al, 1969).

Fama, Fisher, Jensen, and Roll (1969) proposed the concept of event study by conducting seminal researches in this field as early as more than thirty years ago. Since then, event study methodology has been a hot topic and many researchers have employed this approach to evaluate the effects of information disclosure on the firms' security prices. The event study has many applications. In the field of accounting and finance, event studies are employed to analyze the effect of various firm and industry specific events, such as mergers and acquisitions (M&A), issues of new debt or equity, company earnings announcements, stock splits, initial public offering (IPO), etc (Mackinlay, 1997). Chan-Lau (2001) evaluates the effect of restructuring announcements on the stock prices before and after the Commercial Rehabilitation Law (CRL) enactment and observes the advancement in market credibility of restructuring announcements. Jarrell et al (1985) argue that the recalls of drugs and automobiles have a significantly negative influence against corporations' market value. Hendricks et al (1996) assess the effect of quality award winning announcements on firms' market value and come to the conclusion that winning a quality award and disclosing it to the public can produce positive abnormal returns. However, applications also abound in other realms. In the field of economics, Schwert and William (1981) evaluate the effect of changes in the regulatory environment on corporations' market value. Telang and Wattal (2005) employ event study methodology to investigate vendors' incentives to present more secure software. The results demonstrate that vulnerability disclosures cause a negative and significant decrease in the market value to the software vendor. A vendor, on average, suffers from 0.6% decrease in the stock price, which amounts to $0.86 billion in terms of market capitalization values per vulnerability announcement. Mark and Tu (2005) use event study analysis to estimate the impact of center renovation and expansion on shops' retail sales, and observe that adding entertainment facilities to the mall contributes only marginally to the growth of shops' sales inside it; therefore, it is not worth renovating and expanding the mall. In the field of information systems, Subramani et al (2001) employ event study methodology to demonstrate that e-commerce announcements render significantly positive cumulative abnormal returns

(CAR) for corporations. In the realm of information security, Cavusoglu et al (2002) conduct the empirical research at an aggregate level and derive the result that security breach announcements, on the whole, benefit the market of information security and increase their overall market value. Telang and Wattal (2004) argue that vulnerability disclosure announcements indeed render significantly negative CARs for specific software vendors. Acquisti, Friedman, and Telang (2006) argue that the effect of data breaches on the market value of corporations is significantly negative on the announcement day for the security breaches. CARs tend to follow a somewhat peculiar pattern by first increasing and then declining across days after the announcement day. Anyway, no matter what the applications are, the objective is essentially the same - to investigate the effect of a given event on the prices of firms' securities, that is, the market value of a corporation.

To the best of our knowledge, while many of the abovementioned researches provide important insights into the field of economics of information systems, it seems that none of them directly touches government enforcement or analyzes its effect on hackers' behaviors. The goal of this paper is to fill this void by investigating the effect of government enforcement on hackers' behaviors, that is, whether it significantly prevents hackers from further launching security attacks. It complements the existing body of research in the area of empirical studies of information security and serves as an excellent proof to related economic modeling endeavors. In this paper, my contribution is to adopt the event study methodology in the context of information security to assess the effect of government enforcement on hackers' behaviors. Our rationale for applying event study analysis to this scenario is as follows: though it might be impossible to directly evaluate the impact of government enforcement on hackers' behaviors, it is feasible to assess whether or not the decision to enforce a stricter punishment towards hackers is considered as a significant deterrent to hackers. Due to the substantial costs related to government enforcement, it can be viewed as a major event with potential policy as well as financial implications. In addition, since government enforcement is often announced to the public in a high profile, it receives considerable media coverage and public attention. Accordingly, hackers tend to take into consideration the announcements of government enforcement and weigh the benefits against the costs concerning whether it is worthwhile to render security breaches in the future. These considerations should be reflected in the number of security breaches hackers launch. Therefore, investigating the cumulative abnormal returns (CAR) of the number of security attacks due to the intervention of government enforcement allows us to assess hackers' perceptions of the efficacy of the enforcement implemented by the government.

4.2 Methodology

Event study methodology depends on two assumptions. The first assumption is Fama (1970)'s famous efficient market hypothesis (EMH), which argues that current security prices reflect all the information, including market, public, and even private information. According to this line of reasoning, it is only unanticipated events such as government policy and corporate announcements that will enable investors to acquire superior profits. The second point assumes that a reasonable and valid pricing mechanism exists for researchers to gauge whether a given event exerts a significant impact on the dependent variables under consideration. Besides, the mechanism withstands a variety of empirical studies and proves to be correct in most, if not all, researches.

4.2.1 Original Use in Finance and Accounting Research

To start with, it is worthwhile to briefly outline the main procedures of an event study. The classic event study processes defined in the application of finance research are as follows:

1) Define the event of interest, and decide the event date as well as the period over which stock prices associated with this specific event will be investigated.
2) Identify financial returns of individual corporations in the context of no event.
3) Measure the effect of the event by calculating the difference between observed

returns (with event) and expected returns (no event) for each corporation - the difference is called abnormal returns.

4) For each specific corporation, given the event window, aggregate the abnormal returns across time.
5) Determine whether the event has a significant impact by statistically testing the aggregated abnormal returns with one test statistics.

In the finance research, there are abundant methods to compute the normal return of a specific security. The methods can be roughly divided into two groups: statistical and economic approaches. Models in the former category just employ statistical approaches to assess the asset returns and do not take into considerations the economic elements at all, while those in the latter group depend more than on statistical assumptions and use economic models as well (Mackinlay, 1997). For ease of implementation and estimation, only statistical approaches are employed as the underlying model for event study analysis in this paper.

<u>Models</u>

A) Constant Mean Return Model

One of the simplest models might be the constant mean return model, which takes the following form:

$$R_{it} = \mu_i + \varepsilon_{it}\,, \qquad E(\varepsilon_{it}) = 0\,, \qquad \mathrm{var}(\varepsilon_{it}) = \sigma^2_{\varepsilon_i}$$

where R_{it} is the return of stock i at time t, ε_{it} is the error term of stock i at time t with zero expectation and variance $\sigma^2_{\varepsilon_i}$, and μ_i is denoted as the mean return for stock i. The abnormal return for the stock of firm i at period t, ε_{it}, is defined as: $\varepsilon_{it} = R_{it} - \mu_i$. Simple though the model is, it is robust and often produces similar results to those of other complicated models (Brown and Warner, 1980, 1985). The reason is that the variance of the abnormal return tends not to diminish a lot with a more sophisticated model (Mackinlay, 1997). But, since the market model to be discussed later is more widely employed and often yields better results while not adding much to the complexity of the model, we decide to adopt it instead.

B) Market Model

The market model marks a significant improvement to the constant mean return model by explicitly separating the part of the return that is associated with the fluctuations in the market return, thereby reducing the variance of the abnormal return. The advantage of this model is the enhanced capability of statistical tests and a higher probability to detect the effect of a given event. The market model can be represented as follows, which is a little bit similar to the formula of capital asset pricing model (CAPM) in finance research:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it}, \qquad E(\varepsilon_{it}) = 0, \qquad \mathrm{var}(\varepsilon_{it}) = \sigma^2_{\varepsilon_i}$$

where R_{it} and R_{mt} are the normal (expected) returns of stock i and the market assets at period t, and ε_{it} is the error term of stock i at time t with zero expectation and variance $\sigma^2_{\varepsilon_i}$. The abnormal return for the stock of firm i at period t, ε_{it}, is then defined as: $\varepsilon_{it} = R_{it} - \hat{\alpha}_i - \hat{\beta}_i R_{mt}$. EMH assumes that the disturbance term ε_{it} is a random variable with zero mean and the difference between observed and normal returns of stock i at period t should not be significantly different from zero, if there is no major event occurring during that period of time. To check whether abnormal returns exist due to a given event, we just need to test the null hypothesis that the cross-sectional mean of ε_{it} is zero. Any significant difference from zero implies some portion of observed returns that cannot be accounted for by market fluctuations and indeed captures the impact of the specific event. In practice, the market assets R_{mt} employ such indices as the S&P Index, the CRSP Value Weighted Index, etc., depending on whether the stock under consideration is listed on NYSE or NASDAQ.

4.2.2 Adaptation of Event Study Analysis to Our Setting

The traditional procedures and models of event study methodology are illustrated above. Next, we would like to adapt the processes in the finance research to our scenario - economics of information security.

4.2.2.1 Econometric Model

(A) Model Variables

(I) Dependent Variable

The dependent variable of interest is hackers' behaviors, which involves many aspects such as hackers' attacking patterns (Honeynet Project, 2003), hackers' motivations to launch security attacks (Sterling, 1992; Post, 1996; Denning, 1998; Taylor, 1999; Voiskounsky and Smyslova, 2003; Lakhani and Wolf, 2005), and the number of attacks launched by hackers (Browne, McHugh, Arbaugh, and Fithen, 2000, etc.). In this paper, we mainly focus on just one facet of hackers' behaviors - the number of attacks launched by hackers. A larger number of security attacks exhibits more aggressive behaviors indicating unfavorable information security environment, while a smaller number of attacks implies milder actions taken by hackers and correspondingly more favorable security condition. It should be noted that the number of attacks calculated by the Internet Storm Center (ISC) is limited to those that meet a certain severity threshold. In other words, those attacks that do not incur great losses to users are not counted by the ISC. Apart from this limitation, the number of attacks recorded by the ISC includes most of the general security attacks committed by hackers and is therefore considered to be a key variable that characterizes hackers' behaviors from an important perspective.

(II) Independent Variables

Unemployment Rate

The monthly standardized unemployment rate calculated by the Bureau of Labor Statistics of each country represents the number of the unemployed who actively seek jobs but are unable to find jobs as a percentage of the whole labor force. Discouraged workers who do not have a job but do not make efforts to find a new one are not counted as unemployed or as part of the labor force. The unemployment rate is a key indicator of the general social and economic condition. When the economy is gaining momentum, the unemployment rate tends to be low and it is relatively easy for a person who needs a job to find one. On the other hand, when the economy is in recession or stagnating, the unemployment rate tends to be high and a person who wants to land a job may experience much trouble finding one. The resulting outcome might involve crime, increased poverty, political instability, mental health problems, etc. Recent empirical studies have lent much support to the hypothesized positive relationship between unemployment and total suicide rate (Chuang and Huang, 1997; Brainerd, 2001; Neumayer, 2003). Brenner (1979) indicates that increasing unemployment tends to raise the whole crime rate, suicide rate, and leads to worse health conditions. Unemployment implies fewer economic opportunities, reducing the individual's expected income level and thus increasing the possibility of committing crimes. Therefore, the unemployment rate is considered to be an important variable that affects peoples' behaviors. Generally speaking, it is hypothesized that when the unemployment rate is at a high level, more people will be laid off, thus increasing the likelihood of committing crimes including computer hacking. On the other hand, lower unemployment rate usually helps prevent mass poverty and violence, thereby decreasing the odds of committing crimes such as hacking activities. An unemployment rate ranging from 4% to 6% is thought of as "healthy". However, unemployment also, to some extent, benefits the entire economy in the sense that it keeps inflation from reaching a high level and allows employers to identify the employees who are more suitable to the jobs offered. But more often than not, lower unemployment rate is more desirable from the perspective of both society and individuals; therefore, it is hypothesized in our paper that the unemployment rate is positively related to hackers' behaviors - the number of attacks launched.

Government Enforcement

Government enforcement involves the implementation of information security legislation to prevent misuses and exploits of information technology. It serves to promote the general welfare and helps to create a stable environment for a sound economy (U.S. Constitution, preamble). The United States has consistently been a leader in the development and enforcement of information security legislation to gain a clear understanding of the problems facing the information security area and identify corresponding punishments for the individuals as well as organizations that are unable to meet the requirements in the U.S. crime laws. The general U.S. computer crime laws include the Computer Fraud and Abuse Act of 1986 (CFA Act), Communications Decency Act of 1996 (CDA), Computer Security Act of 1987, Gramm-Leach-Bliley Act of 1999 (GLB), National Information Infrastructure Protection Act of 1996, U.S.A. Patriot Act of 2001, etc (Whitman and Mattord, 2003). Of course, other countries including United Kingdom, China, and Germany are following U.S. lead to carry out effective government enforcement to control information security crimes.

It is generally acknowledged that government enforcement has a significantly negative impact on hackers' behaviors - when a government carries out more severe enforcement against hackers, the number of security attacks tends to decrease, while when a government conducts milder enforcement towards hackers, the number of security attacks is expected to increase. Therefore, government enforcement is considered to be the event of interest that has a profound influence on hackers' behaviors. However, to the best of our knowledge, government enforcement has never been directly researched or subjected into empirical testing before. The goal of our paper is to fill this void by measuring the effect of government enforcement on hackers' behaviors.

To illustrate the distinctive impact of enforcements of different magnitude, government enforcement can be further divided into two categories: (1) Prison enforcement such as prison sentence, imprisonment, etc., represented by EJAIL, and (2) Non-prison enforcement such as fines in restitution, hours of community service, deprivation of using the Internet for a specified period of time, etc., denoted by ENOTJAIL. However, in the case of event study methodology, since we can only measure the overall effect of one event at a given time point, government enforcement is treated as a variable that incorporates both prison and non-prison enforcement. In our further research, government enforcement will be separated into two parts to further address the respective effects of prison and non-prison enforcement.

Vulnerability Notes

Vulnerability is defined as a technical flaw or weakness in a system's design, implementation, or operation and management that can be exploited to violate the system's security policy (SANS Institute, 2006). Vulnerability notes have two-fold effects on hackers' behaviors. On the one hand, the disclosure of vulnerability notes provides strong incentives for software vendors to release patches as early as possible and improve the security of their products (Pond, 2000), thus helping to create a sound information security environment and rendering it profitless for hackers to further launch security attacks. The outcome is hypothesized to be a decreasing number of attacks committed. On the other hand, since vulnerability notes involve not only descriptions and impact of a variety of vulnerabilities but also their corresponding solutions and exploits, they provide hackers with a good opportunity to "reverse-engineer" the process and launch security attacks. Besides, although vulnerability disclosure motivates vendors to patch more rapidly, a remarkable portion of users still do not fix the patches appropriately or in time (Arora and Telang, 2005). However, hackers are aware of the vulnerabilities and the chance of exploits now, which motivates them to take advantage of this opportunity to conduct hacking activities, thus leaving end-users in a precarious state. Therefore, it might be socially undesirable and does not necessarily improve overall information security (Elias, 2001; Farrow, 2000). Actually, the ultimate impact of vulnerability notes on hackers' behaviors depends on the interaction and balances of theses two competing effects. Anyway, regardless of the final positive or negative effect, vulnerability notes are considered to be a key variable that affects hackers' behaviors.

Since vulnerability notes include a variety of security attacks or compute-related exploits, it is worthwhile to classify them into different categories so as to assess the respective effects of various vulnerability notes disclosure on hackers' behaviors.

Fadia (2006) presents a good summary of the most common attacks exploited by hackers across the world, which includes: DoS attacks, IP spoofing attacks, Password cracking attacks, Windows attacks, UNIX attacks, Trojan attacks, Keylogger attacks, Input validation attacks, Buffer overflows, Log file hacking, etc. Based on this classification and the vulnerability notes on the websites of SecurityFocus and CERT/CC, we decide to categorize vulnerability notes into three major groups: (a) security breaches due to DoS and DDoS, represented by VDoS, (b) security breaches due to Buffer Overflow, marked by VBUFFER, and (c) security breaches due to other attacks, such as IP Spoofing Attacks, Windows Attacks, Input Validation Vulnerabilities, etc., denoted by VOTHERS. These three categories of vulnerability notes can be considered as *control variables* in the model in the sense that they remain constant for different countries.

(B) Model Form

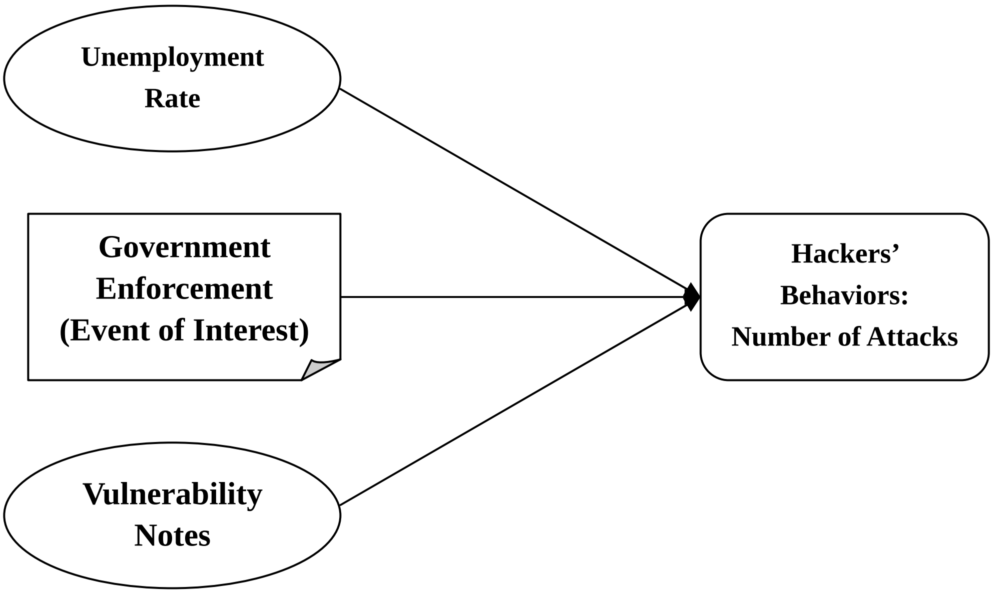
Unemployment Rate
Government Enforcement (Event of Interest)
Vulnerability Notes
Hackers' Behaviors: Number of Attacks

Figure 4.1: Variables Affecting the Hackers' Behaviors

Given the model in Figure 4.1, hackers' behaviors characterized by the number of security attacks for country i at period t are modeled as:

$$No\_Attack_{it} = \beta_i + \alpha_1 UR_{it} + \alpha_2 VD_{it} + \alpha_3 VB_{it} + \alpha_4 VO_{it} + \varepsilon_{it}$$

For simplicity, for a given country, the model can be described as:

$$No\_Attack_t = \beta + \alpha_1 UR_t + \alpha_2 VD_t + \alpha_3 VB_t + \alpha_4 VO_t + \varepsilon_t$$

where No_Attack_t is the daily number of attacks committed by the hackers in the absence of the event in time t; UR_t is the monthly unemployment rate of the country; VD_t is the number of vulnerability notes due to DoS attacks; VB_t is the number of vulnerability notes due to Buffer Overflow; and VO_t is the number of vulnerability notes due to other security attacks. The form is a bit like the market model in finance and accounting research. Since the objective of this paper is to investigate the effect of government enforcement, it is self-evident that government enforcement (event of interest) should not appear in the model of event study methodology. The abnormal return is therefore represented as:

$$\begin{aligned} AR_t &= Observed\_No\_Attack_t - Expected\_No\_Attack_t \\ &= R_t - \hat{\beta} - \hat{\alpha}_1 UR_t - \hat{\alpha}_2 VD_t - \hat{\alpha}_3 VB_t - \hat{\alpha}_4 VO_t \end{aligned}$$

Actually, it is easy to observe that the abnormal return is the error term of the model calculated using out-of-sample (simulation) data which will be discussed in detail in the later sections. Details of data sources and their definitions are to be addressed in the next section.

4.3 Data Sources and Definitions

4.3.1 Dependent Variable

The Number of Attacks (Daily)

For the dependent variable - the number of attacks, data are collected from the country reports of the Internet Storm Center (ISC) at SANS Institute. The country reports on the ISC are generated based on the outputs of DShield sensors (www.dshield.org). Since the aim of this paper is to assess the effect of government enforcement on hackers’ behaviors at the country level, the countries of interest should be first identified. As the ISC only lists countries which are among the top 20 in the world attacked by hackers, we need to make sure that the data are available for all the countries investigated on every sampling day. Now comes the question: if we include more countries in the country list, we can have a broader view of the situations of security breaches across countries, but the more the countries are incorporated, the lower the probability that the data are available for all those countries on the website on any sampling day. Therefore, there is a tradeoff between the number of countries involved and the available data for the number of attacks for all the countries included. Since the ISC includes the country reports for the number of attacks from 2004/1/1 to the present time, we plan to collect data from 2004/1/1 to 2006/8/1, which spans more than two and a half years and contains more than 900 observations. But due to some technical problems associated with the ISC, the actual number of observations is only about 600 at most for a given country. In addition, since it is only comparable when all the countries included are sampled on the same day, this will further reduce the number of observations. The reasonable threshold is assumed to be around 300 sampling days. Therefore, we first select such countries that have more than 300 observations during that period of time (Please see Table 4.1) and then further choose countries that have data available on every sampling day by using Java network programming to automatically extract available data from the ISC. As a result, BE (Belgium) is eliminated from the country list; therefore, the final list of countries involved includes: AU (Australia), BR (Brazil), CA (Canada), CN (China), DE (Germany), ES (Spain), FR (France), GB (United Kingdom), IT (Italy), JP (Japan), KR (Korea), NL (Netherlands), PL (Poland), SE (Sweden), TW (Taiwan), US (United States) - 16 countries in all. The ultimate number of sampling days is just 300, fulfilling the threshold assumption. The start day is 2004/1/5 and the end day is 2006/7/26, and the intervals between any two sampling days are not necessarily the same. For example, the sampling days take the following form: 2004/1/5, 2004/1/7, 2004/1/11, 2004/1/23, … , 2006/6/20, 2006/6/22, and 2006/7/26.

US	**DE**	**CN**	**JP**	**TW**	**KR**	**FR**	**AU**	**BE**
559	562	570	558	556	559	561	559	309
BR	**CA**	**ES**	**GB**	**IT**	**NL**	**PL**	**SE**	
558	572	561	559	519	528	516	413	

Table 4.1: List of Countries that Have Data on More Than 300 Sampling Days

4.3.2 Independent Variables

(A) Standardized Unemployment Rate (Monthly)

Standardized unemployment rate is sampled monthly and collected from various data sources. Actually, it is quite hard to find the data for all of these 16 countries on a monthly basis, but we still manage to collect almost all the data properly. For European Union countries such as Germany, Sweden, Spain, Poland, Italy, France, United Kingdom, and Netherlands, and some other economically powerful countries such as Japan and USA, we can use the automatic bulk downloads on the Eurostat (http://ec.europa.eu/index_en.htm) to gather data; for Australia and Canada, we can log on to OECD (http://www.oecd.org/home/) to collect data; for Korea, Korean National Statistical Office (http://www.nso.go.kr/eng/index.html) provides an excellent data source for our project; for Taiwan, Monthly Bulletin of Statistics compiled by the National Statistical Bureau of Taiwan is used to collect data of unemployment rate; and finally for China, data are collected from the publication of China Monthly Economic Indicators.

(B) Government Enforcement (Daily)

Government enforcement is the event of interest and mainly deals with the arrest, conviction, sentence, fines, or compulsory community service of hackers by the government. We consulted major newspapers for announcements of government enforcement between 2004/1/1 and 2006/8/1, and finally identified Factiva as the main data source. Factiva is an electronic newspaper subscribed by National University of Singapore (NUS) Digital Library, which provides essential business news and information from a wide variety of sources such as the Wall Street Journal, the Financial Times, Dow Jones and Reuters, and also provides strong search engines for access to this rich content collection. The database settings are defined as follows: **Source:** All Sources; **Company:** All Companies; **Subject:** All Subjects; **Industry:** All Industries; **Region:** All Regions; **Language:** English or Chinese-Traditional or Chinese-Simplified. We use the following search keywords: hack* and (convict* or sentenc* or prosecut*). Besides, we also conducted a thorough search of other newspapers and Internet resources such as Google to search for any leakage of government enforcement towards hackers that is somehow not included in Factiva by keying in the search keywords: hack* and (convict* or sentence* or prosecut*) and (every country name) to make the list of events more complete. A typical event of government enforcement might be like this: "A 21-year-old Indiana member of a hacking gang was sentenced to 21 months in prison for breaking into Defense Department computers, federal law enforcement officials said" (reported by CMP TechWeb, 12 May 2005). Another thing that needs to be noted is that an event might be reported by several newspapers, to avoid redundancy of the effects, we simply count as valid the first source for such event, and discard later reports. Table 4.2 lists the number of events for each country. As can be seen from the table, the number of events varies dramatically from country to country.

AU	**BR**	**CA**	**CN**	**DE**	**ES**	**FR**	**GB**
0	1	3	15	1	2	0	8
IT	**JP**	**KR**	**NL**	**PL**	**SE**	**TW**	**US**
0	3	2	1	0	0	0	25

Table 4.2: The Number of Events for Each Country

(C) Vulnerability Notes (Daily)

For the vulnerability notes, data are collected from two main security websites - CERT/CC (www.cert.org) and SecurityFocus (www.securityfocus.com). The former website has a section called Vulnerability Notes Database, which provides descriptions, impact, as well as solutions of a variety of vulnerabilities, while the latter website has a part named Vulnerabilities that offers a complete list of info, discussion, exploit, solution, and references of various vulnerabilities. To measure the respective effects of different categories of vulnerability notes, they are further divided into three major groups: vulnerabilities caused by DoS, Buffer Overflow, and other forms of security attacks. The final values for vulnerability notes are aggregated across the two websites for each of the three categories.

A summary of descriptive statistics of the independent and dependent variables is reported in Table 4.3.

Variables	Source	Mean	Median	Max	Min	Std. Dev.
#_of_Attack	Internet Storm Center	$1.45*10^{6}$	$6.19*10^{5}$	$1.74*10^{7}$	$2.35*10^{4}$	$2.34*10^{6}$
Unemploy. Rate	OECD, Eurostat, etc.	7.13%	6.10%	19.80%	3.20%	3.46%
EJAIL	Factiva	$8.54*10^{-3}$	0.00	1.00	0.00	$9.20*10^{-2}$
ENOTJAIL	Factiva	$5.83*10^{-3}$	0.00	1.00	0.00	$7.61*10^{-2}$
VDoS	CERT/CC, SecurityFocus	1.40	1.00	31.00	0.00	2.42
VBuffer	CERT/CC, SecurityFocus	1.45	1.00	20.00	0.00	2.24
VOthers	CERT/CC, SecurityFocus	8.99	7.00	134.00	0.00	11.26

Table 4.3: Descriptive Statistics of Variables

In addition, the correlation matrix is presented in Table 4.4 in order to measure the strength and direction of the relationships among different independent variables and between independent and dependent variables.

	UR	EJAIL	ENOTJAIL	VDoS	VBuffer	VOthers	#_of_Attack
UR	1						
EJAIL	-0.048^{**}	1					
ENOTJAIL	-0.054^{**}	0.260^{**}	1				
VDoS	-0.011	0.025	0.011	1			
VBuffer	-0.003	0.026	0.006	0.477^{**}	1		
VOthers	-0.025	0.025	-0.004	0.0756^{**}	0.587^{**}	1	
#_of_Attack	-0.177^{**}	0.171^{**}	0.122^{**}	-0.022	-0.014	-0.034^{*}	1

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Table 4.4: Correlation Matrix for Dependent and Independent Variables

As seen from the table, the correlations among different independent variables are quite low, which seems to indicate that multicollinearity between predictors is not a potential problem. However, the test of correlation suffers from several limitations: 1) There are no hard rules to stipulate how high the correlations between predictors are when multicollinearity exists, and 2) Correlation fails to detect the multicollinearity among more than two variables due to the method itself. Therefore, to confirm the previous result, more formal methods should be employed. Here, we adopt the variance inflation factor (VIF), which is the inverse of an independent variable's unique variance that cannot be explained by the rest of the predictors. In other words, VIF measures how much the variance of the estimated regression coefficient increases if the independent variables are correlated with each other. According to the rule of thumb, when VIF is greater than 5 - 10, then the regression coefficient is considered to be poorly estimated. Table 4.5 shows the results of VIF tests for every independent variable. As seen from the table, none of the VIFs is larger than 5, which implies the nonexistence of multicollinearity.

Variables	**UR**	**EJAIL**	**ENOTJAIL**	**VDoS**	**VBuffer**	**VOthers**
VIF	1.005	1.075	1.075	2.345	1.533	2.765

Table 4.5: The Results of VIFs for Every Independent Variable

4.4 Procedures to Apply Event Study Analysis to Our Setting

In this section, the steps to apply event study methodology are discussed in great detail both technically and practically in the context of our paper. The major procedures and statistical inferences mainly follow those in Mackinlay (1997)'s introductory paper.

Step 1: Since the objective of this paper is to investigate the effect of government enforcement on hackers' behaviors, the event of interest is government enforcement, whether in the form of prison enforcement such as conviction and sentence or in the form of non-prison enforcement including fines and compulsory community service hours. The event date is the day when government enforcement is first disclosed to the public. Next, it is essential to specify explicitly the period of interest also known as the event window. The smallest event window is one day - the day when the event takes place. But in reality, the event window is often set to be larger than one to better capture the effect of the event after the announcement day and also to facilitate the application of cumulative abnormal returns (CAR) around the event day. Furthermore, days before the event day are also incorporated in the analysis to account for any information leakage concerning the event. In this research, for the sake of better measuring the aggregate effect of the event, we decide to expand the size of the event window to 15, composed of 7 pre-event days, one event day, and 7 post-event days.

Step 2: The model in our paper is represented by:

$$Expected\_No\_Attack_t = \hat{\beta} + \hat{\alpha}_1 UR_t + \hat{\alpha}_2 VD_t + \hat{\alpha}_3 VB_t + \hat{\alpha}_4 VO_t$$

The number of security attacks can be identified using this equation in the absence of the enforcement variable. Next, it is necessary to specify the length of the estimation window. The longer the estimation window, the more accurate the coefficients can be derived from the estimation equation. However, there exists a tradeoff: larger estimation window tends to reduce the number of events that can be used to conduct event study methodology. In addition, given the fact that generally unemployment rate is cyclical within one year, one year is long enough to serve as the period of the estimation window. For each event, since, from 2004/1/1 to 2004/12/31, there are a total of 68 sampling days for all the countries, the 68 sampling days prior to the event window are used as the estimation window. Therefore, the estimation window is from $t-75$ to $t-8$ and the event window is from $t-7$ to $t+7$. Figure 4.2 illustrates the time line for the whole event study (The event day is day 0). Note that, sometimes, some researchers also create the post-event window after the event window, but whether it is worthwhile to do so depends on the actual situation under investigation.

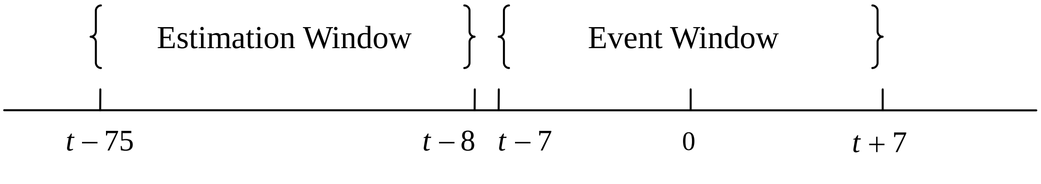

Figure 4.2: Time Sequence for the Whole Event Study

Since the estimation window is set to be 68, only events that occur after 2004/12/31 can be employed to measure their effects on hackers' behaviors. The final number of events for each country is summarized as follows: 0 events for Australia, 0 events for Brazil, 3 events for Canada, 15 events for China, 0 event for Germany, 2 events for Spain, 0 events for France, 6 events for United Kingdom, 0 events for Italy, 3 events for Japan, 2 events for Korea, 1 event for Netherlands, 0 event for Poland, 0 event for Sweden, 0 event for Taiwan, and 17 for United States.

Also, there exists the problem of sampling days vs. calendar days. Since event study methodology is designed based on calendar days, while we just take into account sampling days; therefore, we should redefine the event window in terms of sampling days. For instance, Figure 4.3 gives the time sequence for the real situation in our setting. For the specific event, there are only three sampling days in the 15-day event window. Therefore, we can only accumulate CARs for these three days and calculate their corresponding variance. Actually, the largest event window is 15 days and the actual event window depends on how many sampling days there are in 15 continuous days around the event day. But for simplicity and ease of exposition, we use the $[T_0 - 7, T_0 + 7]$ event window only when illustrating the main steps. When it comes to computing the CARs and their corresponding variances, we will still employ the actual event window.

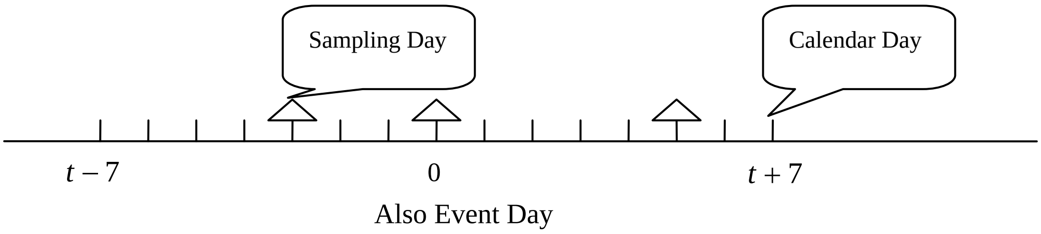

Figure 4.3: Time Sequence for the Real Situation

Step 3: First, supposing that the four basic assumptions are fulfilled, ordinary least squares (OLS) is a best linear unbiased estimator (BLUE) to calculate the coefficients for the model. For a specific country, the OLS estimators for an estimation window of observations during the period from $T_0 - 75$ to $T_0 - 8$ (The event day is assumed to be T_0) can be derived quite easily. After obtaining the coefficients for the estimation window, the expected number of attacks can then be calculated by plugging in the coefficients into the model for the event window (quite similar to the Forecast function in EViews) during the period from $T_0 - 7$ to $T_0 + 7$.

$$Expected\_No\_Attack_t = \hat{\beta} + \hat{\alpha}_1 UR_t + \hat{\alpha}_2 VD_t + \hat{\alpha}_3 VB_t + \hat{\alpha}_4 VO_t$$

Data for the observed number of attacks are collected directly from the data on the ISC. The abnormal return - the difference between the observed number of attacks and the expected number of attacks - is denoted as:

$$\begin{aligned} AR\_No\_Attack_t &= Observed\_No\_Attack_t - Expected\_No\_Attack_t \\ &= R_t - \hat{\beta} - \hat{\alpha}_1 UR_t - \hat{\alpha}_2 VD_t - \hat{\alpha}_3 VB_t - \hat{\alpha}_4 VO_t \end{aligned}$$

The null hypothesis assumes that the abnormal returns are jointly normally distributed with a zero mean and variance $\sigma^2(AR\_No\_Attack_t)$. Before we use specific statistics to test the hypothesis, it is necessary to aggregate the abnormal returns first.

Step 4: For each country, given the event window, the abnormal returns are aggregated across time. The reason why abnormal returns should be aggregated is to draw overall inferences for the event under investigation. Actually, the aggregation should be conducted across two dimensions: 1) across time, and 2) across all the events taking place in a given country. First, we aggregate the abnormal returns across time for a given event i during the event window, and the result is called cumulative abnormal returns (CAR), which can be expressed as:

$$CAR_i(T_0 - 7, T_0 + 7) = \sum_{t=T_0-7}^{T_0+7} AR_{it}$$

When the length of the estimation window increases, in an asymptotical sense, the variance of CAR_i is:

$$\sigma_i^{\,2}(T_0-7,T_0+7)=((T_0+7)-(T_0-7)+1)\sigma_{\varepsilon_i}^{\ 2}=15\sigma_{\varepsilon_i}^{\ 2}$$
$$=15/(68\text{-}5)\cdot\sum_{t=T_0-75}^{T_0-8}(R_t-\hat{\beta}-\hat{\alpha}_1UR_t-\hat{\alpha}_2VD_t-\hat{\alpha}_3VB_t-\hat{\alpha}_4VO_t)^2$$

Therefore, the distribution of the CAR is described as:

$$CAR_i(T_0-7,T_0+7)\sim N(0,\sigma_i^{\,2}(T_0-7,T_0+7))$$

The above distribution is just applicable to the condition of one event. But since only one event is incapable of characterizing the overall effect of such events for a particular country, it is essential to aggregate the events within one given country. Given M events, the average CARs (ACAR) across the events are calculated as:

$$\overline{CAR}(T_0-7,T_0+7)=\frac{1}{M}\sum_{i=1}^{M}CAR_i(T_0-7,T_0+7)$$

$$\text{var}(\overline{CAR}(T_0-7,T_0+7))=\frac{1}{M^2}\sum_{i=1}^{M}\sigma_i^{\,2}(T_0-7,T_0+7)$$

Therefore, after a two-dimensional aggregation, the distribution of the ACAR is:

$$\overline{CAR}(T_0-7,T_0+7)\sim N[0,\text{var}(\overline{CAR}(T_0-7,T_0+7))]$$

Step 5: Determine whether the event has a significant effect by statistically testing the ACAR with one test statistics. The null hypothesis H_0 can be verified using the following statistics:

$$\theta=\frac{\overline{CAR}(T_0-7,T_0+7)}{\text{var}(\overline{CAR}(T_0-7,T_0+7)^{1/2}}\sim N(0,1)$$

The criterion is that if the p-value is less than 0.05 (Sometimes, the threshold can be extended to 0.1), then government enforcement (event of interest) is considered to have a significant effect on hackers' behaviors, which provides important policy as well as economic implications. Note that the test statistics is asymptotic with respect to the length of the estimation window and the number of events. In other words, the more the number of events and the larger the estimation window, the more accurate the result is. In this paper, ACAR is also interpreted in another term, that is, **average enforcement impact**. Although we use z statistic to test the hypothesis, it does not mean there is only one test that can perform such task. Actually, a variety of test statistics are available to conduct it. Brown and Warner (1985) provide a comprehensive introduction of appropriate test statistics for measuring the effect of the event. Interested readers can also consult Patell (1976) on the tests based on standardization.

4.5 Data Analysis and Empirical Results

Now we present the empirical results of the event study analysis here. To ensure data quality, a data cleansing procedure was performed after the data were collected. The process is based on the criterion that there are no missing data for each country under investigation. After data cleansing, we can use the standard event study methodology to measure the effect of the event. The estimation window is from $T_0 - 75$ to $T_0 - 8$ and the event window is from $T_0 - 7$ to $T_0 + 7$ (The event day is assumed to be T_0).

4.5.1 Event Study Results

Table 4.6 presents the results that investigate the effect of government enforcement on hackers’ behaviors for each individual country after taking into account the difference between sampling days and calendar days. In other words, sampling days are used to measure the effect of government enforcement, and the event window is correspondingly revised to meet this purpose.

The jargon average CAR in finance research is interpreted in another term - **average enforcement impact**, which shows the average difference between the observed number of attacks (in the presence of the event) and the predicted number of attacks (in the absence of the event) across all events occurring within one specific country. As seen from the table, government enforcement has a significant impact against hackers’ behaviors by dramatically reducing malicious attacks launched by hackers with the absolute value ranging from $1.13*10^6$ (Netherlands) to $1.60*10^7$ (Spain) and p-value varying from 0.0082 (Netherlands) to 0.0000. The effect of government enforcement varies from country to country. The impact on Canada, China, Spain, United Kingdom, Korea, and United States is extremely statistically significant

Country	**No. of Events**	**Event Date**	**Average Enforcement Impact* (p-value)**
CA	3	2005.01.06; 2005.11.17; 2006.01.17.	$-2.20*10^6$ (0.0000)***
CN	15	2005.03.21; 2005.03.23; 2005.07.11; 2005.07.12; 2005.10.19; 2005.11.08; 2005.11.14; 2005.11.15; 2005.11.18; 2006.02.24; 2006.04.10; 2006.04.15; 2006.04.22; 2006.04.27; 2006.05.12.	$-1.18*10^7$ (0.0000)***
ES	2	2006.02.07; 2006.04.08.	$-1.60*10^7$ (0.0000)***
UK	6	2005.01.30; 2005.10.10; 2005.11.05; 2005.12.30; 2006.01.17; 2006.05.10.	$-2.44*10^6$ (0.0000)***
JP	3	2005.03.25; 2005.04.14; 2005.11.10.	$-1.36*10^6$ (0.0042)**
NL	1	2005.10.10.	$-1.13*10^6$ (0.0082)**
KR	2	2005.7.12; 2006.05.21.	$-3.36*10^6$ (0.0000)***
US	17	2005.01.29; 2005.02.25; 2005.03.14; 2005.10.14; 2005.10.22; 2005.12.30; 2006.01.28; 2006.04.13; 2006.04.21; 2006.05.06; 2006.05.09; 2006.05.10; 2006.05.11; 2006.05.16; 2006.05.25; 2006.06.08; 2006.06.09.	$-9.40*10^6$ (0.0000)***

***** Significant at the 0.1 percent level (p<0.001)**

**** Significant at the 1 percent level (p<0.01)**

*** Significant at the 5 percent level (p<0.05)**

Table 4.6: The Effect of Government Enforcement for Each Country

(p<0.001), while the impact upon Japan and Netherlands is very statistically significant (p<0.01). The fact that the effect of government enforcement for Japan is not as remarkable as that for other countries might be accounted for by the following reasons: Japanese companies, on average, are relatively slower to establish and implement managerial measures, such as employee education and policy clarification, since only around 23 percent of them have set up formal information security policies. In addition, it seems that most Japanese companies rely too heavily on software such as firewalls, anti-virus applications and intrusion detection systems, but neglect what, in essence, is the most effective kind of countermeasures, "people measures" also known as soft issues (Kunii, 2001) - a point quite consistent with Anderson (1993)'s that information security breaches are caused largely by the misinstallation, misconfiguration, and mismanagement of people rather than the failure of the technology or system itself. Furthermore, for some political reasons, the home pages of many Japanese companies are frequently broken into by some organized hackers such as a Chinese hacker organization called the Honker Union of China (HUC) (Please refer to http://www.cnhonker.com, 2001). And to make matters worse, Japanese government fails to effectively impose strict enforcement against those hacker groups, which is one of the main reasons for the not-so-remarkable effect of government enforcement. Therefore, Japanese government should take appropriate measures and exercise further efforts to address its information security from the above perspectives, and contributes to the establishment of sound information security. Of course, those countries with extremely statistically significant p-values should not slacken and should maintain their efforts in addressing their information security issues, and continue to take advantage of effective government enforcement to combat hacking activities. On the whole, government enforcement proves to be associated with significant negative and deterrent effects against the number of attacks committed by hackers, which is consistent with our expectations (The term of average enforcement impact is negative in sign, and all p-values are significant at least at 1 percent level).

Next, the length of the event window is extended to 22 days, which is composed of 7 pre-event days, one event day, and 14 post-event days. The objective of this research is to investigate whether the effect of government enforcement will decay or diminish in extent as time goes by. Of course, another possibility is that as the amount of the observation days (event window) increases, certain delayed effects of government enforcement will take place anew or even become more remarkable, which further impacts against hackers' behaviors. The rationale for using this asymmetric event window rather than the orthodox symmetric one is that post-event days tend to capture much more important and meaningful information including the impact of the event than pre-event days do. The pre-event days might include more "noise" or irrelevant information especially with the extension of the event window. Therefore, pre-event days should not be considered of the same importance and weight as post-event days. Thus, we decide to properly expand the length of the post-event days to 14 days while simultaneously maintaining the size of the pre-event window that involves seven days in order to eliminate the phenomenon of irrelevant noise information. Table 4.7 presents the comparisons of the results for the two different sizes of event windows: 15 days and 22 days, respectively. As can be seen from the table, for Canada, China, United Kingdom, Korea, and United States, the effect of government enforcement decays dramatically with the increase of the length of the event window, which might be explained as follows: Although government enforcement seems to be quite severe in these countries as can be seen from the very statistically significant p-values in the table, these countries are still subject to heavy hacking activities - due to economic, political or other potential reasons - as time passes by. Besides, the decayed effect is consistent with human's common sense and our expectations, and thus desirable. However, for countries such as Spain and Netherlands, the effect of government enforcement intensifies rather than decays as the event window increases from 15 days to 22 days, which means that government enforcement has a delayed effect against hackers' behaviors. It might be caused by the fact that the disclosure mechanisms of these two countries are not very effective to release enforcement announcements to the public, thus rendering people including hackers uninformed of the enforcement cases or informed much later than they should be. As for countries like Japan, the effect of government enforcement is influenced by a combination of these two forces - decayed effect and delayed effect. And the final outcome is a mixture of these two effects with neither one dominating or eliminating the other. In addition, some CARs for certain countries change from previously hypothesized negative values to positive values, which implies that hackers' behaviors are basically not impacted on those days far away from the event day.

Country	**No. of Events**	**15-day Event Window**				**22-day Event Window**			
		AEI[10]	**SD**[10]	**theta**[10]	**p**	**AEI**	**SD**	**theta**	**p**
CA	3	$-2.20*10^6$	$5.38*10^5$	-4.10	0.0000^{***}	$-1.86*10^6$	$6.13*10^5$	-3.03	0.0024^{**}
CN	15	$-1.18*10^7$	$1.05*10^6$	-11.27	0.0000^{***}	$-4.66*10^6$	$1.22*10^6$	-3.80	0.0001^{***}
ES	2	$-1.60*10^7$	$1.19*10^6$	-13.48	0.0000^{***}	$-3.02*10^7$	$1.46*10^6$	-20.69	0.0000^{***}
UK	6	$-2.44*10^6$	$2.43*10^5$	-10.06	0.0000^{***}	$-2.03*10^6$	$2.89*10^5$	-7.03	0.0000^{***}
JP	3	$-1.36*10^6$	$4.75*10^5$	-2.86	0.0042^{**}	$-1.40*10^6$	$5.47*10^5$	-2.58	0.0099^{**}
NL	1	$-1.13*10^6$	$4.25*10^5$	-2.64	0.0082^{**}	$-3.01*10^6$	$6.03*10^5$	-4.99	0.0000^{***}
KR	2	$-3.36*10^6$	$5.75*10^5$	-5.85	0.0000^{***}	$-9.89*10^5$	$6.27*10^5$	-1.58	0.1145
US	17	$-9.40*10^6$	$1.47*10^6$	-6.41	0.0000^{***}	$-5.54*10^6$	$1.81*10^6$	-3.06	0.0022^{**}

***** Significant at the 0.1 percent level (p<0.001)**

**** Significant at the 1 percent level (p<0.01)**

*** Significant at the 5 percent level (p<0.05)**

Table 4.7: Comparisons between Different Event Windows

In order to further illustrate our results, we plan to measure the magnitude of the effect of government enforcement on the number of attacks. The average daily number of attacks for each country is calculated by making a summation of the number of attacks during the 300 sampling days and then averaging it. After coping with the denominator, we will next handle the numerator. Since the average

[10] AEI denotes average enforcement impact, while SD represents standard deviation. Theta is a test statistics indicating the extent of the effect of government enforcement, which is equal to average enforcement impact divided by standard deviation.

enforcement impact deals with a window composed of several sampling days, it is necessary to "average" the number as follows. Take, the average enforcement impact for Canada, for example. Canada has three events with 10, 11, and 11 sampling days, respectively, in the 15-day event window. The average sampling days are $(10+11+11)/3 \approx 11$. Then the average enforcement impact is divided by 11, which derives the numerator. The magnitude of the effect of government enforcement is calculated as follows:

$$\left|\frac{\text{Average enforcement impact / Average sampling days}}{\text{Average daily number of attacks}}\right| \times 100\%$$

Table 4.8 summarizes the magnitude of the effect of government enforcement for each country. As seen from this table, the magnitude of the effect varies dramatically from country to country with the largest being 84.66% (Spain) and the smallest being 10.12% (U.S.). Most of the values are within the range from 19% to 43%, which indicates a remarkably negative effect of government enforcement on hackers' behaviors. The result that the magnitude of the effect for U.S. is the lowest among all the countries under investigation is beyond our expectations. U.S has always been a leader in the development and enforcement of information security legislation to promote the general welfare and create a stable information security environment for a sound economy. But why does its government enforcement have the slightest impact against hackers' behaviors? The reason might be that U.S. firms and individuals are subject to a high chance of security attacks due to some reasons such as economic benefits, political revenge, etc., in spite of its strict enforcement against hackers. In other words, hackers tend to believe that the benefits of attacking U.S. firms or individuals outweigh the corresponding costs, thus it is worthwhile to launch attacks.

Next, we consider the global magnitude of the effect of government enforcement, which is approximated by the following formula below Table 4.8:

Country	No. of Events	Average Enforcement Impact	Average Sampling Days	Average Number of Attacks	Magnitude of the Effect of the Event
CA	3	$-2.20*10^6$	11	$1.03*10^6$	19.42%
CN	15	$-1.18*10^7$	11	$3.28*10^6$	32.71%
ES	2	$-1.60*10^7$	10	$1.89*10^6$	84.66%
UK	6	$-2.44*10^6$	10	$6.95*10^5$	35.11%
JP	3	$-1.36*10^6$	8	$7.27*10^5$	23.38%
NL	1	$-1.13*10^6$	7	$4.33*10^5$	37.28%
KR	2	$-3.36*10^6$	10	$7.91*10^5$	42.48%
US	17	$-9.40*10^6$	10	$9.29*10^6$	10.12%

Table 4.8: The Magnitude of the Effect of Government Enforcement for Each Country

$$\left| \frac{\sum_{i=1}^{8} \frac{\text{Average enforcement impact}}{\text{Average sampling days}} / 8}{\sum_{1}^{8} \text{Average daily number of attacks}/8} \right| \times 100\%$$

After some calculation, the result is 28.32%, which means government enforcement has a 28.32% deterrent effect on hackers' behaviors at a global level. Therefore, government enforcement proves to be associated with significant negative effects against the number of security attacks committed by hackers on a global basis, which is quite consistent with our expectations. However, it should be noted that the global claim is limited in the sense that the values only takes into consideration eight typical countries all over the world. Future researches might consider including more countries to further evaluate the validity of the results.

Furthermore, Table 4.9 presents specific values for the CAR on the event day. The important property of this table is that it involves both the mean and median abnormal returns across all events on the event day T_0. The difference is defined as $\left|(\text{MedianAR} - \text{MeanAR}) / \text{MeanAR}\right|$. As seen from the table, on the event day, both statistics are negative and significant as expected. However, these two values are not equal to each other most of the time (Since there are only two events for Spain and Korea and one event for Netherlands, their means and medians are necessarily the same). As for Japan, the difference is up to 146.42%, which indicates the presence of strong outliers that drive the mean to them and away from the rest of the points and it might endanger the robustness of the estimators. Fortunately, except that of Japan, the difference between mean and median abnormal returns for other countries is within an acceptable range with the largest no more than 40%.

CAR (t=0)	**Canada**	**China**	**Spain**	**United Kingdom**
Mean AR	-160315	-1178405	-564005	-292033
Median AR	-170472	-932247	-564005	-182928
Difference(%)	6.34%	20.89%	0%	37.36%
CAR (t=0)	**Japan**	**Korea**	**Netherlands**	**United States**
Mean AR	-27207	-270756	-1030223	-1118503
Median AR	-67044	-270756	-1030223	-1193126
Difference(%)	146.42%	0%	0%	6.67%

Table 4.9: Mean and Median Abnormal Return on the Event Day

4.5.2 Implications for Theory and Practice

This study provides important implications for both theory and practice. From the theoretical perspective, first of all, this study adapts event study methodology from the finance research to the field of information security and successfully employs it to investigate the impact of government enforcement against hackers’ behaviors, which demonstrates that government enforcement indeed has a significantly negative and deterrent effect on hackers’ behaviors as expected. On the one hand, it indicates that event study analysis can be successfully extended to research fields in addition to finance and accounting, and used to derive desirable results. On the other hand, it complements the existing body of research in the area of information security by incorporating an important variable - government enforcement - and makes a step towards a more comprehensive model of information security that is useful for policy making adopted by the government. In addition, our results can be used to serve as an empirical proof of the proposition that hackers' targeting decreases as the enforcement rate increases presented in Png, Tang, and Wang (2006). Our results are also somewhat comparable to those found in Hui and Png (2003), which argues that the demand for the pirated information products is decreasing as the expected penalty increases. The proposition is similar to our viewpoint that as government enforcement enhances, the number of security attacks launched by hackers decreases. Chen and Png (2003) develop a theoretical model that takes into consideration the interactions among government policy, the producer's business strategy, and users' choices. Their key result is that government policies that center on penalties alone will be socially sub-optimal. The result seems to somewhat contradict with our stance, but considering the different scenarios, we think it is possible to combine these two seemingly contrasting conclusions. Becker (1968) constructs a theoretical economic model to measure the optimal public and private policies to combat illegal behaviors. The main contribution of his paper is to indicate that the optimal government policy to combat illegal behaviors is a matter of the optimal allocation of social resources. Our study can follow his lead and conduct empirical analysis to test whether the so-called "optimality conditions" hold using real-world data. Future researches can extend our study by constructing a more complicated econometric model, basing it on certain sophisticated underlying economic model, and collecting more recent data sources to better measure the effect of government enforcement on hackers' behaviors.

From the perspective of practice, our results also provide valuable directions that can guide governments to take more strategic and rational actions. The results show that government enforcement has a significantly negative impact against hackers' behaviors. The magnitude of its effect varies greatly from country to country within the range from 19% to 43% except two countries - Spain (84.66%) and the U.S.A. (10.12%). That means U.S.A. should exercise further efforts and take more active measures to deter hackers from launching security attacks although it is taking the lead in developing and implementing computer crime laws to promote a sound information security environment. In addition, government enforcement has a negative 28.32% deterrent effect on hackers' behaviors at a global level. Therefore, the government can properly convict or prosecute hackers in the form of prison terms, probation, fines, compulsory community service hours, etc., to deter them from committing cyber-crimes if it wants to create a sound information security atmosphere.

4.5.3 Regression Analysis

The previous event study analysis mainly focuses on measuring the effect of government enforcement from the perspective of each individual country. To extend the scope of our research, we conduct a regression analysis to evaluate the overall effect of government enforcement that takes into account all the countries under investigation. In this section, we employ panel data methods to assess the overall picture of the effect of government enforcement.

Actually, panel data which have relatively few cross-sections, with variables listed in cross-section specific individual series are called "pooled time series, cross-section data" in contrast to ordinary panel data with a large number of cross-sectional units (QMS, 2004). But, to avoid confusion, these two terms are used interchangeably in the following sections. Panel data or longitudinal data typically refer to data containing time series observations of the same units (individuals, households, firms, etc.). Therefore, observations in panel data generally involve two dimensions - cross-sectional dimension, denoted by subscript i, and time series dimension, marked by subscript t. Two widely used panel data sets in economics are the National Longitudinal Surveys of Labor Market Experience (NLS) and the University of Michigan's Panel Study of Income Dynamics (PSID) (Hsiao, 2003). Panel data possess several major advantages over traditional pure cross-sectional or pure time-series data sets (Hsiao, 1985). The most obvious advantage is that panel data tend to increase the sample size, which increases the degrees of freedom and reduces the multicollinearity among explanatory variables, thus improving the accuracy and efficiency of parameter estimates, and enables the researchers to specify more complicated models. In addition, panel data allow the researchers to control for individual, unobservable heterogeneity that might cause biases in estimation results. The third advantage is that the use of panel data makes it possible to address many important economic questions unanswerable by either a cross-section or a time-series alone. Finally, panel data might help eliminate or diminish estimation biases. Given the above advantages of panel data, it is worthwhile to employ such methods even at the cost of more complex model specification, estimation, and data analysis.

4.5.3.1 Econometric Model

(A) Model Variables

The variables in the model are almost the same as those used previously except that some independent variables are further classified into smaller groups.

The dependent variable of interest is hackers' behaviors, which is represented by the number of security attacks launched by hackers.

The first independent variable deals with unemployment rate, which is standardized and collected on a monthly basis. The second independent variable is government enforcement, which is treated as a binary variable, with 1 indicating the presence of the event and 0 the absence of the event. To further illustrate the distinctive impact of enforcements of different magnitude, government enforcement is divided into two categories: (1) Prison enforcement such as prison sentence, imprisonment, etc., represented by EJAIL, and (2) Non-prison enforcement such as fines in restitution, hours of compulsory community service, deprivation of using the Internet for a specified period of time, etc., denoted by ENOTJAIL. Each category is represented by an independent binary variable. Since now panel data estimation rather than event study methodology is employed, the variable - government enforcement (now two independent categories) - can and should appear in the estimation equation. The third independent variable involves the disclosure of vulnerability notes, which are further classified into different groups - VDoS, VBUFFER, and VOTHERS - so as to assess their respective effects of various vulnerability notes disclosure on hackers' behaviors.

(B) Model Form

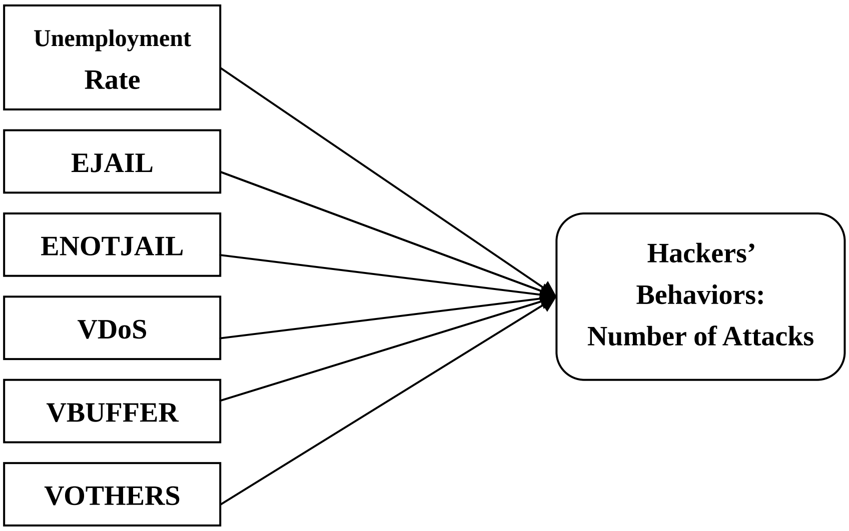

Figure 4.4: Variables Influencing the Hackers' Behaviors

Econometric Framework

Given the model in Figure 4.4, using the subscripts i and t to denote the country and sampling day, the baseline specification to be estimated is modeled as:

$$No\_Attack_{it} = \alpha_i + X'_{it}\beta + \varepsilon_{it} = \alpha_i + \beta_1 UR_{it} + \beta_2 EJAIL_{it} + \beta_3 ENOTJAIL_{it}$$
$$+ \beta_4 VDoS_t + \beta_5 VBUFFER_t + \beta_6 VOTHERS_t + \varepsilon_{it}$$

$$i = 1, \cdots, N. \quad t = 1, \cdots, T.$$

where No_Attack_{it} is the daily number of security attacks launched by the hackers across 16 countries and over 300 sampling days, X_{it} is a vector of explanatory variables constructed from empirical findings that includes UR_{it} - the monthly unemployment rate of country i on day t, $EJAIL_{it}$ - a binary variable that equals 1 if prison enforcement exists in country i on day t, $ENOTJAIL_{it}$ - another binary variable that equals 1 if non-prison enforcement occurs in country i on day t,

$VDoS_t$ - the number of vulnerability notes caused by DoS attacks for all the countries on day t, $VBUFFER_t$ - the number of vulnerability notes caused by Buffer Overflow for all the countries on day t, and $VOTHERS_t$ - the number of vulnerability notes caused by other forms of attacks for all the countries on day t. The model assumes that there is no reverse causation, which can be verified using *Granger Causality* test (Granger, 1969). $\beta(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6)$ are unknown parameters to be estimated and ε_{it} is the error term that varies across individual countries and over time. The parameter α_i denotes unobservable country specific fixed effects - heterogeneity. This parameter controls for individual factors that vary across countries but are time invariant within specific countries, which might involve lifestyles, traditions, ideology, geography, personal interests and preferences that may influence hackers' behaviors but fail to be captured by the explanatory variables in the baseline model.

The data source is exactly the same as that for the event study analysis; therefore, I will not elaborate it here.

4.5.3.2 Empirical Results

We employ the fixed effects model (FEM) to estimate the coefficients of the model. The main advantage of the FEM lies in its relative ease of parameter estimation and that the independence of the individual fixed effects from the other explanatory variables is not mandatory, e.g., $E[X \cdot \alpha_i] \neq 0$. The major disadvantage is that it requires the estimation of N separate intercept coefficients, which is costly in terms of degrees of freedom (Baltagi, 2001). The problem is particularly acute when N is large and T is small. However, fortunately, it does not pose a problem to our research, since N is 16 (small) and T is 300 (large) in our scenario. Of course, we could also use the random effects model (REM) to estimate the coefficients. The main strength of the

REM results from its economic use of degrees of freedom in the estimation, thus making it more efficient than the FEM. The main weakness of the model is the strict assumption that the random effects are independent of the involved explanatory variables, e.g., $E\left[X \cdot \alpha_i\right] = 0$. It is plausible that certain unobservable effects not incorporated in the model might be correlated with the independent variables. This violation of the assumption may lead to inconsistent results and biases in the β vector. Whether to treat the individual effects α_i as fixed or random is no easy question to answer, which has generated a heated debate in the biometrics, statistics, and econometrics literature (Baltagi, 2001). Generally, the determination can be implemented by using a statistical test called Hausman test, which tests for the null hypothesis that X and α_i are uncorrelated. If the null hypothesis is rejected indicated by a significant difference between the two estimators, it favors the FEM and rejects the REM. Otherwise, it is advised to continue to employ the REM.

<table>
<tr><td colspan="4">Correlated Random Effects - Hausman Test
Pool: POOLBASELINE
Test cross-section random effects</td></tr>
<tr><td>Test Summary</td><td>Chi-Sq. Statistic</td><td>Chi-Sq. d.f.</td><td>Prob</td></tr>
<tr><td>Cross-section random</td><td>0.000000</td><td>6</td><td>1.0000</td></tr>
</table>

Table 4.10: The Results of the Hausman Test

Table 4.10 presents the outcome of the Hausman test. The p-value (p = 1.000 > 0.05) is insignificant, which indicates that the null hypothesis should not be rejected and; therefore, REM seems to be more appropriate in this scenario. However, other researchers (e.g., Hsiao, 1985, 2003) argue that the result given by the Hausman test is exploratory rather than confirmatory and the choice of the FEM over the REM might depend on the nature of the particular problem. For instance, if the cross-sectional units deal with countries, large companies or industries, it may be more appropriate to assume that the unobservable effects are fixed (FEM) and not generated by a random draw from the population. On the other hand, if we are coping with individuals or other small entities drawn from a large population, the assumption of REM is more reasonable. Since, in our scenario, the cross-sectional units denote countries, we should use the FEM. But considering the insignificant p-value derived by the Hausman test, we should then use the REM. Therefore, to achieve a delicate balance between these two opposite conclusions, I decide to present both results and let the readers decide by themselves.

To demonstrate the advantages of the FEM and the REM, another estimation model - pooled ordinary least squares (OLS) estimation - is also presented here. The model is as follows:

$$y_{it} = \alpha + X^{'}_{it}\beta + \varepsilon_{it} \qquad i = 1,\cdots,N.\ t = 1,\cdots,T.$$

Table 4.11 presents the outcomes of the FEM, REM, and pooled OLS estimation. As seen from Column 2, the FEM derives the best results: The adjusted R-square is 0.856787, which is quite acceptable. The p-values for the unemployment rate ($0 < 0.01$) and vulnerability notes due to other forms of attacks ($0.001 < 0.01$) are extremely statistically significant, and the p-value ($0.0481 < 0.05$) for prison enforcement is very statistically significant. In addition, they have the desirable signs as hypothesized. The results show that unemployment rate has an encouraging effect on hackers' behaviors and prison enforcement exerts a deterrent impact against hackers' behaviors. The negative sign of VOTHERS indicates that the disclosure of vulnerability notes caused by other forms of attacks provides strong incentives for software vendors to release patches as early as possible and improve the security of their products, which outweighs the force that hackers use vulnerability notes to "reverse-engineer" the process and launch security attacks. Therefore, the outcome is a deterrent effect on hackers' behaviors. However, non-prison enforcement has an undesirable positive sign. To matter matters worse, it is statistically significant with a wrong sign, which claims that non-prison enforcement actually encourages hackers to engage in hacking activities. One plausible reason might be that non-prison enforcement such as fines in restitution, hours of compulsory community service, and deprivation of using the Internet for a specified period of time might be considered as too light or mild to constitute a real deterrent factor to hackers. As hackers render substantial financial losses to the victims due to security breaches, they are expected to experience severe punishment which is at least proportional, if not more, to the severity of their hacking activities. However, unfortunately, in the field of information

Parameters	**FEM**	**REM**	**Pooled OLS**
Const	764929.3 (6.618439)	1105158 (7.443704)	2274430 (28.52293)
UNEMPLOYMENTRATE	102579.2*** (6.461266)	55273.19*** (3.899273)	-111811*** (-11.9749)
EJAIL	-288283** (-1.97689)	-227059 (-1.55739)	3657801*** (9.953876)
ENOTJAIL	739023.9*** (4.238243)	764310*** (4.383501)	2302402*** (5.183728)
VDOS	3758.301 (0.465012)	4842.671 (0.599315)	5450.844 (0.264068)
VBUFFER	6633.955 (0.936318)	7846.271 (1.107825)	9069.325 (0.501512)
VOTHERS	-7552.43*** (-3.97494)	-8248.98*** (-4.34827)	-10534.4** (-2.18441)
Adjusted R^2	0.856787	0.813074	0.063851
F-statistic	1368.165	1100.595	55.55361
Number of observations	4800	4800	4800

***** Significant at the 1 percent level (p<0.01), ** Significant at the 5 percent level (p<0.05)**

*** Significant at the 10 percent level (p<0.10), The values in the parenthesis are t-values for the parameters.**

Table 4.11: The Empirical Results for the FEM, REM, and Pooled OLS

security, the severity of the punishment is at a low level currently (e.g., Hollinger, 1991; Michalowski and Pfuhl, 1991). For example, Brett Edward O'Keefe, a hacker, who hacked into government and private computers including the U.S. Army and NASA and resulted in substantial financial losses within the range of $95,000 to $100,000, only faced a negligible 60-day work-release program and 100 hours of community service as a result of pleading guilty (The San Diego Union-Tribune, 2nd Aug. 2005). It is hard to believe such light non-prison enforcement will have a profound deterrent impact against hackers, who might think since legal punishment is not severe at all, the benefits of launching hacking activities still outweigh the corresponding costs and it is worthwhile continuing to commit hacking - the ultimate effect might be a counterproductively encouraging instead of discouraging impact against hackers' behaviors. Of course, whether this tentative explanation is tenable or not is itself an issue of empirical analysis and thus entails further investigation. However, the fact that the previous hypothesis that it should have a significant negative sign later evolves into a significant positive (wrong) sign is, after all, outrageous and beyond our wildest expectations, which implies the baseline model leaves much to be desired. Later, I will address this problem by slightly modifying the estimation procedure.

In addition, VDOS and VBUFFER are not statistically significant because it is influenced by two opposing forces: 1) Strong incentives for software vendors to release patches as early as possible and improve the security of the products, and 2) Hackers use solutions in vulnerability disclosure to “reverse-engineer” the process and further commit hacking activities. The result indicates that for vulnerability notes due to Denial of Service (DoS) and Buffer Overflow, neither force dominates or eliminates the other, thus leading to the insignificant t-values. Another possible explanation might be that the classification of vulnerability notes into three groups (e.g., DoS, BUFFER, and Others) fails to capture the effect of vulnerability notes on hackers' behaviors - perhaps, the classification is too general to be of much use or hackers' behaviors are indeed not affected much by vulnerabilities due to DoS attacks and Buffer Overflow.

Column 3 in Table 4.11 presents the results of the REM. On the whole, the results of the REM are almost similar to those of the FEM. The p-values for unemployment rate (0.0001 < 0.01) and vulnerability notes due to other forms of attacks (0 < 0.01) are extremely statistically significant, and the p-value ($0.1194 \approx 0.10$) for prison enforcement is nearly statistically significant at the 10% level. The results indicate that unemployment rate exerts an encouraging effect on hackers' behaviors and prison enforcement has a deterrent impact against hackers' behaviors. The negative significant sign of VOTHERS indicates that the disclosure of vulnerability notes caused by other forms of attacks actually encourages software vendors to address information security more seriously and rapidly, which offsets the effect that hackers take advantage of the disclosure to launch more security attacks. However, the undesirable positive sign of non-prison enforcement similar to that of the FEM seems to reject our hypothesis.

Column 4 in Table 4.11 presents the results of pooled OLS estimation. The results are quite unsatisfactory: unemployment rate, prison enforcement, and non-prison enforcement have the unintended signs, especially all with statistically significant p-values. In addition, the adjusted R-square is 0.063851, which is very low and unacceptable. The main reason for the poor estimation is that pooled OLS estimation austerely assumes the intercepts and slope coefficients are homogeneous across all N cross-sections and over all T time periods, which discards the temporal dimension - “within variation” - and space dimension - “between variation” and simply throws away much useful information. Therefore, I will mainly use the FEM in the later panel data estimation.

The highlighted items in Table 4.11 indicate the presence of unintended estimation results that are contrary to our hypotheses. To remedy this problem, we propose three approaches to address this issue. First, the rolling window method is employed. The procedure is described as follows: aggregate the data in the 7-day rolling window and implement the FEM:

$$\begin{aligned}\sum No\_Attack_{it}/7 &= \alpha_i + \beta_1\sum UR_{it}/7 + \beta_2\sum EJAIL_{it}/7 + \beta_3\sum ENOTJAIL_{it}/7 \\ &\quad + \beta_4\sum VDoS_t/7 + \beta_5\sum VBUFFER_t/7 + \beta_6\sum VOTHERS_t/7 + \varepsilon_{it}\end{aligned}$$

$$i = 1,\cdots,N. \qquad t = 1,\cdots,T.$$

The rationale is that since end-users need some time to fix the patches, it is not likely they will patch the vulnerabilities on a daily basis; instead, it may be more reasonable to assume that they fix the patches weekly. Therefore, we try to estimate the model using a rolling window consisting of 7 days. The second approach is nearly the same as the baseline model except that we just extract weekly samples from 300 sampling days. For example, we draw the samples with the observation number 1, 8, 15, …, 295 to assess the weekly effect; therefore, there are 43 observations for each country. Third, since the data for all the variables are collected on a daily basis except that the data for the variable, unemployment rate, are gathered monthly, because only monthly unemployment rate is available. Therefore, it poses the issue of incompatible sampling intervals among predictors and response variables, which might compromise the validity of the empirical results derived from the model. To address this issue, we attempt to collect the data for all the variables, independent or dependent variables, on a monthly basis, and then implement the FEM. To be more specific, the data for the number of security attacks, vulnerability notes including VDoS, VBuffer, and VOthers are aggregated across the whole month. The data for unemployment rate are just left unchanged, since it is already at a monthly level. And finally, government enforcement including EJAIL and ENOTJAIL is again treated as a binary variable, which equals 1 if the corresponding enforcement occurs within the month under investigation. One additional advantage of this approach is that it enables the event to take place more frequently at the monthly level. It is highly plausible that there are a sporadic number of events occurring on a daily basis but quite a few events taking place on a monthly basis. The aggregation at the monthly level tends to increase the number of value 1’s for the binary enforcement variable, which might increase the validity of the results, since the test statistics is asymptotic with respect to the number of events.

Parameters	Model 1	Model 2	Model 3	Model 4
Const	764929.3 (6.618439)	9053679 (12.62215)	-161635 (-0.39939)	-534363.5 (-0.038461)
UNEMPLOYMENT RATE	102579.2*** (6.461266)	397719.3*** (4.259694)	224253.3*** (3.944485)	1631267.7 (0.899707)
EJAIL	-288283** (-1.97689)	-1371282*** (-4.842)	-632010* (-1.65820)	-19800838*** (4.695067)
ENOTJAIL	739023.9*** (4.238243)	2980528*** (8.391399)	-28853.8 (-0.06493)	809139.1 (0.182442)
VDOS	3758.301 (0.465012)	27186.69 (1.838062)	-3616.59 (-0.16329)	-195841.8 (-1.412167)
VBUFFER	6633.955 (0.936318)	16985.76 (1.248526)	-5413.88 (-0.32228)	221552.9* (1.733167)
VOTHERS	-7552.43*** (-3.97494)	-35691.7*** (-10.9718)	3237.388 (0.604392)	51008.46** (2.224691)
Adjusted R^2	0.856787	0.903648	0.86593	0.753555
F-statistic	1368.165	2101.352	212.2945	48.04959
Number of observations	4800	4704	688	352

***** Significant at the 1 percent level (p<0.01)**

**** Significant at the 5 percent level (p<0.05)**

*** Significant at the 10 percent level (p<0.10)**

The values in the parenthesis are t-values for the parameters.

Table 4.12: The Empirical Results for Four Models Using the FEM

Table 4.12 summarizes the results for the baseline model (Model 1), baseline model with a rolling window (Model 2), baseline model with weekly samples (Model 3), and baseline model with data aggregated on a monthly basis (Model 4), all of which use the FEM. Note that the number of observations for Model 2 is 4704, since the last six rows should not be counted in the rolling window and thus there are 294 entries for each country. As seen from this table, Model 3 best addresses the issue of unintended positive sign of non-prison enforcement in Model 1, Model 2, and Model 4. In addition, the p-value for unemployment rate (0.0001 < 0.01) is extremely statistically significant, and the p-value for prison enforcement ($0.1004 \approx 0.1000$) is nearly statistically significant at the 10% level. The sign of non-prison enforcement is negative as hypothesized, although not significant in the p-value. The adjusted R-square is 0.86593, which is quite acceptable. Finally, none of the p-values for vulnerability notes (DoS, Buffer Overflow, and other forms of attacks) is statistically significant, which can be argued that vulnerability notes have two-fold effects on hackers' behaviors - 1) encouraging software vendors to release patches more rapidly and improve the security of their products and 2) simultaneously providing hackers with a good opportunity to "reverse-engineer" the process and launch security attacks. Actually, the ultimate impact of vulnerability notes on hackers' behaviors depends on the interaction and balances between theses two competing effects. Therefore, Model 3 is a good alternative to be employed as the ultimate model for panel data estimation.

Unit Root Test

Since panel data contains information across countries and over time, the issue of stationarity in time-series should be addressed. A time-series is said to be stationary if its mean and variance are constant over time and the simple correlation coefficient between the two time periods only depends on the length of the lag but not on the actual time when the coefficient is calculated. If one or more of these properties are not fulfilled, it is referred to as nonstationary. The motivation to the research of such question is that if a time series is nonstationary, then it is not possible to generalize the results to other time periods, which limits the practical value of such time series (Gujarati, 2003). The major negative effect of nonstationarity is spurious correlation that tends to inflate adjusted R^2 and the t-values of the nonstationary independent variables (Studenmund, 2001). A test of assessing stationarity that has been gaining popularity in the past few years is the unit root test. Actually, we employ the

Dickey-Fuller test in our research to test for a unit root. To run the Dickey-Fuller test, the following equation is estimated: $\Delta Y_t = \beta_0 + \beta_1 Y_{t-1} + \varepsilon_t$, and one-sided t-test is run with the null hypothesis that $\beta_1 = 0$. If β_1 is significantly less than zero, we can reject the null hypothesis of a unit root - nonstationarity. Of course, we can then run the Dickey-Fuller test for every variable including independent and dependent variables. However, Studenmund (2001) proposes that the presence of nonstationarity indicated by the Dickey-Fuller test does not necessitate changing the functional form of the model. In other words, before modifying the model, cointegration is first employed to check whether it is essential to implement the modification. Cointegration involves matching the degree of nonstationarity of the variables in the equation to make the disturbance term stationary and frees the equation from any spurious correlation. Even if individual variables are not stationary, it is still possible for combinations of nonstationary variables to exhibit stationarity - cointegrated. If individual variables have unit roots but are cointegrated as a whole, then we can still use their original forms (Studenmund, 2001). Therefore, we can directly check the residuals of the equations to test for cointegration using the Dickey-Fuller test.

Table 4.13 presents the results of the cointegration of the residuals of the equations. The p-values for all the countries are statistically significant, which rejects the null hypothesis of unit root and indicates the stationarity of the time-series. Therefore, Model 3 does not need to be modified to address the issue of stationarity in panel data estimation.

4.5.4 Event Study Methodology vs. Panel Data Estimation

In this section, we focus our attention on making comparisons between the results derived using event study methodology and panel data estimation and providing some explanations about certain inconsistent results.

Country	Variable	Coefficient	Std. Error	t-Statistic	Prob.
AU	RES_AU(-1)	-0.38583	0.113684	-3.39389	0.0016***
BR	RES_BR(-1)	-0.75104	0.14594	-5.14624	0***
CA	RES_CA(-1)	-0.58789	0.1899	-3.0958	0.0037***
CN	RES_CN(-1)	-0.41864	0.119957	-3.48993	0.0012***
DE	RES_DE(-1)	-0.29086	0.113201	-2.56941	0.0140**
ES	RES_ES(-1)	-0.36636	0.118041	-3.10365	0.0035***
FR	RES_FR(-1)	-0.62515	0.143642	-4.35213	0.0001***
GB	RES_GB(-1)	-0.41267	0.132577	-3.11266	0.0034***
IT	RES_IT(-1)	-0.46958	0.186668	-2.51561	0.0162**
JP	RES_JP(-1)	-0.33978	0.142813	-2.37922	0.0225**
KR	RES_KR(-1)	-0.28268	0.11034	-2.56192	0.0143**
NL	RES_NL(-1)	-0.55659	0.141803	-3.92512	0.0003***
PL	RES_PL(-1)	-0.22916	0.087466	-2.62002	0.0124**
SE	RES_SE(-1)	-0.4678	0.140026	-3.34081	0.0018***
TW	RES_TW(-1)	-0.50858	0.141067	-3.60527	0.0009***
US	RES_US(-1)	-0.69643	0.147802	-4.7119	0***

***** Significant at the 1 percent level (p<0.01)**

**** Significant at the 5 percent level (p<0.05)**

*** Significant at the 10 percent level (p<0.10)**

Table 4.13: The Empirical Results for the Cointegration of the Residuals

On the whole, empirical results derived by means of event study analysis and panel data estimation concertedly demonstrate that government enforcement has a significantly negative and deterrent effect against hackers' behaviors, and it is worthwhile for governments to remain and enhance enforcement against hackers in order to cultivate a sound information security environment. However, there are also some discrepancies between empirical results using these two methods. In terms of event study methodology, the results are quite satisfactory and desirable. Except for two countries - Japan and Netherlands - that have significant p-values at the 1 percent level, the rest of the countries all have extremely significant p-values at the 0.1 percent level, which indicates a remarkably deterrent effect of government enforcement. In comparison, as for the results derived by panel data estimation, prison enforcement is statistically significant at the 5 percent level, but non-prison enforcement is statistically significant with the undesirable sign. Even after the modification of the baseline model, non-prison enforcement is still insignificant even if the sign is consistent with our hypothesis, which seems to imply that non-prison enforcement does not have a remarkable impact against hackers' behaviors. Therefore, there seems to be some discrepancies between the empirical results using different approaches. After further thoughts, some preliminary explanations are presented to account for the reason why the results using two distinct approaches are, to some extent, inconsistent with each other.

- Event study methodology is a powerful approach that has the capability to isolate the impact of the event within a given period of time. The ability arises through the construction of event window and researchers measure the effect of the event only within the range of this specified event window. Generally, reverberations of the event are still being felt during the relatively small event window compared with the whole time line, which can effectively capture the impact of the event. By contrast, panel data estimation just treats the event of interest as an ordinary binary variable no different from other independent variables. It does not distinguish the differences among event window, estimation window, and other sampling days, and just consider all the sampling days completely the same. The effect of the event might dilute or decay over time due to the indiscriminate handling of sampling days, which fails to capture the effect of the event that may, as a matter of fact, exist. Thus, event study methodology is capable of deriving more statistically significant p-values and capturing the impact of the event more effectively and accurately than panel data estimation.
- Due to some objective reasons related to event study methodology itself, it cannot investigate the effect of two events simultaneously, which is the reason why

government enforcement is treated as a whole. But this variable is categorized into two groups - prison and non-prison enforcement - in panel data estimation. It is highly possible that even though one part of enforcement is significant and the other part is insignificant, the final combination of these two parts as a whole still exhibits significant p-values. Actually, after observing the data for government enforcement, more than 90% belongs to the category of prison enforcement, which shows significant p-values in panel data estimation. Thus, both of the inconsistent results might be considered reasonable in the sense that they just explore the problem from different perspectives but, in essence, might reveal the same answer. Anyway, it is just a tentative explanation of the reason of the inconsistent results. Whether it is valid or not should be examined more carefully in later researches.

- The inconsistency of the results might be caused by different scopes and applicability of the two approaches. Event study methodology measures the effect of government enforcement at an individual country level with different p-values for each country, while panel data estimation examines the effect of the event at a global level with the same p-value for all the countries. In this sense, it is relatively more difficult to derive statistically significant p-values using panel data estimation, and the empirical results dealing with these two different scopes are hard or impossible to make comparisons between each other.
- It seems that event study methodology is less sensitive to the selection of independent variables. The model might suffer from the limitations of omission of relevant variables or inclusion of irrelevant variables. If that is the case, then the validity of the results derived using either of these two approaches is bound to be compromised. However, event study methodology still exhibits excellent empirical results with significant p-values, while panel data estimation is incapable of deriving significant p-values for some variables, which indicates the latter approach might be highly sensitive to the selection of explanatory variables.

On the whole, event study methodology is a little more superior to panel data estimation in our setting in the sense that it is able to isolate the impact of the event within a given period of time and, more importantly, derive more desirable empirical results and capture the impact of the event more effectively. Of course, it does not mean panel data estimation is not useful or worthwhile in this research at all. It also has its own advantages and applicability: e.g., it can measure the effect of government enforcement at a global level that takes into account all the countries under investigation. That is the reason why we take the time and efforts to conduct a complementary empirical analysis using panel data estimation to better illustrate the results given by event study methodology.

4.6 Limitations and Future Research

Notwithstanding the systematic and concerted efforts I have invested in this study, there are still some limitations that may undermine the inference power of my research findings as follows:

First, data for the dependent variable - the number of attacks - are collected from the Internet Storm Center (ISC), which only lists countries that are among the top 20 in the world attacked by hackers. That means the results derived are mainly applicable to “top hacked” countries but may not apply to “less hacked” ones. The main reason is due to the biased sample selection. In addition, the number of events for some countries is quite limited (e.g., there is only 1 event for Netherlands), which might pose a threat to the validity of the final results, since the z test statistics in this scenario is asymptotic with respect to the number of events. Future researches can use more sufficient and recent data to include both “top hacked” and “less hacked” countries and try to find more events for each country, thus producing a more complete picture of security attacks throughout the world.

Second, government enforcement in the event study analysis is assumed to be homogeneous (exogenous), which does not vary in the level of seriousness. However, in reality, a mere $500 fine may provide entirely different implications to hackers compared with a ten-year imprisonment punishment. But, event study methodology in this scenario cannot effectively distinguish the nature of government enforcement such as prison and non-prison punishment simply due to the method itself. To address this problem, we have conducted a complementary regression analysis that distinguishes between prison and non-prison enforcement by using two binary variables in the estimation equation - each one for the respective punishment to evaluate the overall effect of government enforcement that takes into account all the countries under consideration rather than the individual effect at the country level derived using event study methodology. However, the result is not perfectly satisfactory in the sense that the p-value for non-prison enforcement is not statistically significant. Future researches can try to classify government enforcement into smaller groups that vary in the level of seriousness.

Third, in this paper, we only categorize vulnerabilities into three major groups: vulnerabilities caused by DoS, Buffer Overflow, and other forms of security attacks. An important direction for future work is to make a further classification into smaller groups by subdividing vulnerabilities caused by other forms of security attacks. Although it requires more variables to be estimated and more data to be collected, it will provide us with a more comprehensive view of the respective effect of vulnerability notes on hackers' behaviors, which is quite desirable and worthwhile the extra efforts.

Fourth, the statistical insignificance of non-prison enforcement and some vulnerability notes might be caused by the omission of relevant variables. Since the omission of relevant variables leads to biased estimates of the parameters and inclusion of irrelevant attributes only causes inefficient - but still unbiased - estimates, it is advisable to include the irrelevant variables rather than exclude the relevant ones. Further endeavors may incorporate some seemly relevant variables such as GDP, the installed base of internet users for each country, etc., to better assess the relationships between variables. However, as more explanatory variables are included, they may be correlated with the error terms or other independent variables, or may contain measurement errors, thus producing biased and inconsistent estimates. In that case, we have to identify instrumental variables and employ the two-stage least squares (2SLS) approach to estimate the parameters. Of course, it poses a major challenge to find an appropriate instrumental variable that is highly correlated with the model's explanatory variables but uncorrelated with the error term. Sometimes, the procedure of identification itself is an art rather than a science.

Finally, our paper mainly investigates the effect of external factors on hackers' behaviors from one perspective - government enforcement. A meaningful extension of the research involves conducting a study from an internal perspective that measures the impact of users' behaviors against hacking activities. Future researches can look for data sources on users' precautions, e.g., the number of downloads of patches from Microsoft, CERT/CC, SecurityFocus, etc., and subsequently examine the impact against hackers' behaviors. Of course, a major challenge is to acquire sufficient and high-quality data on users' behaviors. To the best of our knowledge, the best source of information and data on users' behaviors are the AOL/NCSA Online Safety Study (Png, Tang, and Wang, 2006). However, the insufficiency of the data, which is collected only twice - in 2004 and 2005, severely compromises its application to the panel data estimation. In addition, due to the shortage of data, we could also consider conducting a smaller empirical study that includes a fewer number of countries under investigation.

Chapter 5 Conclusions

In this paper, a complete literature review of the background of, barriers to, and traditional measures of information security is presented to serve as a solid foundation for further research.

Information security background is illustrated with a lot of figures and statistics collected from various sources. The participants in this field involve four groups of agents that interact with each other - hackers, end-users, software vendors, and security specialists such as CERT/CC. The barriers to sound information security environment are attributable to insufficient incentives that are further categorized into four classes, namely negative network externalities, liability assignment, no accurate measures of information security, and other barriers to information security, with appeal for urgent actions to properly align economic incentives to address this problem.

An extensive literature review points out three main directions of research endeavor in the field of information security, that is, technological approaches, behavioral aspects, and economic approaches to information security. Although technical methods might be the easiest for the organizations to implement and centrally control, it is by no means the most effective (Boss, 2005). As for behavioral approaches, Straub (1990) suggests that behavioral solutions to information security might be more effective than traditional technological ones. However, behavioral ways also face several problems such as generally auxiliary to technical solutions and only concentrating on “either the organization level or management level of effective control design” (Chin, 1999; Rees et al, 2003). Therefore, economic approaches can be employed to address the issue of information security and should play an active role in this field to better align incentives to establish a sound information security environment (Anderson, 2001; Varian, 2000). On the whole, economic methods to information security are further classified into five main streams of research directions, that is, strategic interactions between hackers and end-users, software vulnerability disclosure and patch policies, optimal investment in information security, liability assignment and cyberinsurance, and evaluations of information security technologies. Unfortunately, however, nearly no papers, to the best of our knowledge, have focused on the impact of government enforcement on hackers' behaviors.

To address this problem, this study makes a meaningful attempt to investigate the effect of government enforcement against hackers' behaviors using event study methodology. Our results demonstrate that government enforcement has a significantly negative and deterrent impact against hackers' behaviors by dramatically reducing the number of security attacks launched. The magnitude of the effect of government enforcement varies dramatically from country to country within the range from 19% to 43% except two countries - Spain (84.66%) and the U.S. (10.12%), which indicates a remarkably negative effect of government enforcement on the number of attacks. In addition, government enforcement has a negative 28.32% deterrent effect on hackers' behaviors at a global level. Furthermore, the results given by panel data estimation using the fixed effects model demonstrate that government enforcement especially prison enforcement dramatically influences hackers' behaviors. Therefore, government enforcement proves to be associated with significant negative effects against the number of security attacks committed by hackers either for an individual country or on a global basis, which is quite consistent with our expectations.

The main contributions of this paper are as follows:

- Event study methodology can be successfully extended to the field of information security in addition to the finance and accounting area, and can be used to derive useful results.
- It complements the existing stream of research in the realm of information security by including an important yet untouched variable - government

enforcement - and helps, to some extent, to establish a more sophisticated model of information security that provides important policy as well as economic implications.

- Our results can be used to serve as empirical proofs of some viewpoints proposed by other researchers.
- This study distinguishes between sampling days and calendar days by redefining the event window and adjusting the subsequent procedures to properly compute CARs and corresponding variance, which extends the application of event study analysis to this new scenario.
- The research measures the magnitude of the effect of government enforcement for each individual country as well as at a global level.
- Our results provide important implications that can guide governments to better address the problem of enforcement against hackers and help to create a sound information security environment.

Although we have conducted a relatively complete literature review of the field of information security and performed meaningful empirical studies using event study methodology and panel data estimation, we still think there are a great number of opportunities as well as challenges in this thriving area, especially considering organizations' ever-increasing dependence on information systems for operational, strategic, and e-commerce activities in the current ICE Age. Information security is a nascent, dynamic, and rapidly-developing field, which will be even more promising and prosperous in the near future.

References

[1] Ackerman, M., Cranor, L., and Reagle, J. “Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences”, *Proceedings ACM Conference Electronic Commerce (EC99), ACM Press*, 1999, pp. 1-8.

[2] Acquisti, A., and Grossklags, J. “Privacy and Rationality in Individual Decision Making”, *Security & Privacy Magazine, IEEE, Carnegie Mellon University, Pittsburgh, PA, USA*, 2005, pp. 24-30.

[3] Acquisti, A., Friedman, A., and Telang, R. “Is There a Cost to Privacy Breaches? An Event Study”, *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), 2006.

[4] Agrawal, J., and Kamakura, W.A. “The Economic Worth of Celebrity Endorsers: An Event Study Analysis”, *Journal of Marketing* (59:3), Jul. 1995, pp. 56-62.

[5] Akerlof, G. A. “The Market for ‘Lemons’: Quality, Uncertainty and the Market Mechanism”, *The Quarterly Journal of Economics* (84), Aug. 1970, pp. 488-500.

[6] Amanda, L. “Hacker Attacks Spur Web Liability Products”, *National Underwriter* (104:11), 2000.

[7] Anderson, R. “Why cryptosystems fail”, *Proceedings of the 1st ACM Conference on Computer and Communications Security, Virginia, USA*, 1993, pp. 215- 227.

[8] Anderson, R. “Why Information Security is Hard - An Economic Perspective”, *17th Annual Computer Security Applications Conference, New Orleans, Louisiana*, Dec. 2001.

[9] Anderson, R., and Schneier, B. “Economics of Information Security” (Guest Editors’ Introduction), *IEEE Computer Society, IEEE Security & Privacy*, 2005.

[10] Arora, A., and Telang, R. “Economics of Software Vulnerability Disclosure”, *IEEE Computer Society, IEEE Security & Privacy*, 2005, pp. 20-25.

[11] Arora, A., Forman, M., Nandkumar, A., and Telang, R. “Competitive and Strategic Effects in the Timing of Patch Release”, *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), 2006.

[12] Arora, A., Krishnan, R., Telang, R., and Yang Y. “An Empirical Analysis of Vendor Response to Disclosure Policy”, *H. John Heinz III School of Public Policy and Management, Carnegie Mellon University, Pittsburgh PA*, Mar. 2005.

[13] Arora, A., Telang, R., and Xu, H. “Timing Disclosure of Software Vulnerability for Optimal Social Welfare”, *Carnegie Mellon University, Working Paper*, Apr. 2004a.

[14] Arora, A., Telang, R., and Xu, H. “Optimal Policy for Software Vulnerability Disclosure”, *Carnegie Mellon University, Working Paper*, 2004b.

[15] Ashish, G., Jeffrey, C. et al. “The real cost of being hacked”, *The Journal of Corporate Accounting & Finance* (14:5), 2003.

[16] AT&T. “Network Security: Managing the Risk and Opportunity”, *AT&T Point of View*, Jul. 2004, pp. 1-21.

[17] August, T., and Tunca, T. I. “Network Software Security and User Incentives”, *Unpublished manuscript, Graduate School of Business, Stanford, Revised*, Aug. 2005.

[18] Baer, W. “Rewarding IT Security in the Marketplace”, *Contemporary Security Policy* (24:1), 2003, pp. 190-208.

[19] Ball, L. D. “Computer Crime. In F. Tom”, *The Information Technology Revolution, Cambridge, MA: MIT Press*, 1985, pp. 532-545.

[20] Baltagi, B. H. “Economics of Analysis of Panel Data (2nd edition)”, *John Wiley & Sons, Ltd*, 2001.

[21] Beattie, S., Arnold, S., Cowan, C., Wagle, P., and Wright, C. “Timing the Application of Security Patches for Optimal Uptime”, *In LISA XVI*, Nov. 2002.

[22] Becker, G. S. “Crime and Punishment: An Economic Approach”, *Journal of Political Economy* (76:2), 1968, pp. 169-217.

[23] Ben-Yehuda, N. “Deviance in Science: Towards a Criminology of Science”, *British Journal of Criminology* (26), 1986, pp. 1-27.

[24] Beveren, J. V. “A Conceptual Model of Hacker Development and Motivations”, *Journal of E-Business* (1:2), Dec. 2001, pp. 1-9.

[25] Blakley, B. “An Imprecise But Necessary Calculation”, *Secure Business Quarterly: Special Issue on Return on Security Investment* (1:2), 2001.

[26] Blakley, B. “The Measure of Information Security is Dollars”, *In The First*

Workshop on Economics and Information Security, 2002.

[27] Bloom-Becker, J. “Computer Crime Law Reporter”, *Los Angeles: National Center for Computer Crime Data*, 1986.

[28] Bohme, R. “Cyber-Insurance Revisited”, *The Workshop on the Economics of Information Security* (WEIS 2005), 2005.

[29] Bohme, R., and Kataria, G. “Models and Measures for Correlation in Cyber-Insurance”, *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), 2006.

[30] Boss, S. R. “Control, Risk, and Information Security Precautions”, *ICIS 2005 Doctoral Consortium Abstract, Katz Graduate School of Business, University of Pittsburgh*, 2005.

[31] Brainerd, E. “Economic Reform and Mortality in the Former Soviet Union: a Study of the Suicide Epidemic in the 1990s”, *European Economic Review* (45), 2001, pp. 1007–1019.

[32] Brenner, M.H. “Influence of the Social Environment on Psychology: The Historical Perspective”, *Stress and Mental Disorder*, Raven University Press, New York, 1979.

[33] Brown, S.J., and Warner, J.B. “Measuring Security Price Performance”, *Journal of Financial Economics* (8:3), Sep. 1980, pp. 205–258.

[34] Brown, S.J., and Warner, J.B. “Using Daily Stock Returns: The Case of Event Studies”, *Journal of Financial Economics* (14:1), Mar. 1985, pp. 3–31.

[35] Browne, H. K., McHugh, J., Arbaugh, W. A., and Fithen, W. L. “A Trend Analysis of Exploitations”, *CS-TR-4200, UMIACS-TR-2000-76*, Nov. 2000.

[36] Caelli, W., Longley, D., and Shain, M. “Information Security Handbook”, *London: Macmillan*, 1991.

[37] Camp, L. J., and Wolfram, C. “Pricing Security”, *Proceedings of the CERT Information Survivability Workshop, Boston, Massachusetts*, 2000, pp. 31-39.

[38] Cavusoglu, H., Cavusoglu, H., and Zhang, J. “Economics of Security Patch Management”, *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), 2006.

[39] Cavusoglu, H., Mishra, B., and Raghunathan, S. “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers”, *Working Paper*, 2002.

[40] Chandler, A. “The Changing Definition and Image of Hackers in Popular Discourse”, *International Journal of the Sociology of Law* (24), 1996, pp. 229-251.

[41] Chan-Lau, J.A. “Corporate Restructuring in Japan: An Event-Study Analysis”, *IMF Working Paper*, Dec. 2001.

[42] Chellappa, R. K., and Sin, R. “Personalization Versus Privacy: An Empirical Examination of the Online Consumer’s Dilemma”, *To Be Published in Information Technology and Management* (6:2-3), 2005.

[43] Chen, Y.N., and Png, I. P. L. “Information Goods Pricing and Copyright Enforcement: Welfare Analysis”, *Information Systems Research* (14:1), Mar. 2003, pp. 107-123.

[44] Chin, S. K. “High-Confidence Design for Security: Don't Trust—Verify”, *Communications of the ACM* (42:7), Jul. 1999, pp. 33 – 37.

[45] Choi, J. P., Fershtman, C., and Gandal, N. “Internet Security, Vulnerability Disclosure and Software Provision”, *CEPR Discussion Paper No. 5269*, Oct. 2005.

[46] Chuang, H. L., and Huang, W. C. “Economic and Social Correlates of Regional Suicide Rates: a Pooled Cross Section and Time Series Analysis”, *Journal of Socio-Economics* (26), 1997, pp. 277–289.

[47] Coase, R. H. “The Problem of Social Cost”, *Journal of Law and Economics* (3), 1960, pp. 1-44.

[48] Computer Crime & Intellectual Property Section, *United States Department of Justice*, Available at http://www.cybercrime.gov (Last visited: Nov. 2006).

[49] Computer Science and Telecommunications Board (CSTB), “Cybersecurity Today and Tomorrow”, *Washington D.C., National Research Council*, 2002, p. 7.

[50] “Computer Security-Related Insurance Issues”, *Insurance Information Institute*, Sep. 2003.

[51] Csikszentmihalyi, M. “Beyond Boredom and Anxiety: The Experience of Play in Work and Games”, *San Francisco: Jossey-Bass*, 1977.

[52] Csikszentmihalyi, M. “Finding Flow: The Psychology of Engagement with Everyday Life”, *New York: Basic Books*, 1997.

[53] Csikszentmihalyi, M. “Flow: The Psychology of Optimal Experience”, *New York: Harper & Row*, 1990.

[54] Dacier, M., Pouget, F., and Debar, H. “Honeypots: Practical Means to Validate Malicious Fault Assumptions”, *Proceedings of the 10th IEEE Pacific Rim International Symposium on Dependable Computing* (PRDC’04), 2004, pp. 383-388.

[55] Denning, D. “Information Warfare and Security”, *Reading: Addison-Wesley*, 1998.

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

[57] Dhillon, G. “Principles of Information Systems Security: Text and Cases”, *Wiley*, 2006.

[58] Donner, M. “Patch Management - Bits, Bad Guys, and Bucks!”, *Secure Business Quarterly* (3:2), 2003, pp. 1-4.

[59] Dornseif, M., and May, S. A. “Modeling the Costs and Benefits of Honeynets”, *The Third Workshop on the Economics of Information Security* (WEIS 2004), 2004.

[60] Duff, L., and Gardiner, S. “Computer Crime in the Global Village: Strategies for Control and Regulation—In Defense of the Hacker”, *International Journal of the Sociology of Law* (24), 1996, pp. 211-228.

[61] Elias, L. “Full Disclosure Is a Necessary Evil”, *SecurityFocus.com*, 2001, Available at www.securityfocus.com/news/238 (last visited: Jul. 2006).

[62] European Union, “Network and Information Security: Proposal for a European Policy Approach”, *COM*, 2001.

[63] Fadia, A. “Network Security - A Hacker’s Perspective (2nd Edition)”, *Thomson, Course Technology*, 2006.

[64] Fama, E. F. “Efficient Capital Markets: A Review of Theory and Empirical Work”, *Journal of Finance* (25), 1970, pp. 383-417.

[65] Fama, E. F., Fisher, L., Jensen, M. C., and Roll, R. “The Adjustment of Stock Prices to New Information”, *International Economic Review* (10:1), 1969, pp. 1-21.

[66] Farrow, R., "The Pros and Cons of Posting Vulnerability", *The Network Magazine*, 2000, Available at www.networkmagazine.com/shared/article (last visited: Jul. 2006).

[67] Fisk, M. "Causes & Remedies for Social Acceptance of Network Insecurity", *In The First Workshop on Economics and Information Security*, May 2002.

[68] Frey, B. "Not Just for the Money: an Economic Theory of Personal Motivation", *Brookfield. VT: Edward Elgar Publishing Company*, 1997.

[69] Gohring, N. "Cyberinsurance May Cover Damage of Computer Woes", *Seattle Times*, Jul. 2002.

[70] Gordon, L. A., and Loeb, M. P. "Return on Information Security Investments: Myths vs. Realities", *Strategic Finance*, Nov. 2002, pp. 26-31.

[71] Gordon, L. A., and Loeb, M. P. "The Economics of Information Security Investment", *ACM Transactions on Information and Systems Security*, Nov. 2002, pp. 438-457.

[72] Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson R. "CSI/FBI Computer Crime and Security Survey", *Computer Security Institute*, 2005.

[73] Granger, C. W. J. "Investigating Causal Relations by Econometric Models and Cross-spectral Methods", *Econometrica* (37), 1969, pp. 424-438.

[74] Gujarati, D. N. "Basic Econometrics (4th edition)", *New York: McGraw-Hill*, 2003.

[75] Halbert, D. "Discourses of Danger and the Computer Hacker", *The Information Society* (13), 1997, pp. 361-374.

[76] Hann, I. H., Hui, K. L., Lee, T. S., and Png, I. P. L. "Online Information Privacy: Measuring the Cost-Benefit Trade-off", *Proceedings 23rd International Conference on Information Systems*, 2002.

[77] Hannemyr, G.. "Technology and Pleasure: Considering Hacking Constructive", *Firstmonday, Peer-Reviewed Journal on the Internet* (4:2), 1999.

[78] Hendricks, K.B., and Singhal, V.R. "Quality Awards and the Market Value of the Firm: An Empirical Investigation", *Management Science* (42:2), 1996, pp. 415-436.

[79] Hollinger, R. C. "Hackers: Computer Heroes or Electronic Highwaymen?",

Computers and Society (2), 1991, pp. 6-17.

[80] Honeynet Project. “Know Your Enemy: GenII Honeynets Easier to Deploy, Harder to Detect, Safer to Maintain”, Jun. 2003. Available at http://project.honeynet.org/papers/gen2 (last visited Jul. 2006).

[81] Honeynet Project. “Know Your Enemy: Trend Analysis”, *The Honeynet Project & The Honeynet Research Alliance*, 2004.

[82] Honeynet Project. “Know Your Enemy”, *Addison-Wesley*, 2001.

[83] Hoo, K. J. S. “How Much Is Enough? A Rish-Management Approach to Computer Security”, *Consortium for Research on Information Security and Policy (CRISP)*, Jun. 2000.

[84] Hsiao, C. “Analysis of Panel Data” (2nd Edition), *Econometric Society Monographs, Cambridge University Press*, 2003.

[85] Hsiao, C. “Benefits and Limitations of Panel Data”, *Econometric Reviews* (4:1), 1985, pp. 121-174.

[86] Huang, C. D., Hu, Q., and Behara, R. S. “Economics of Information Security Investment in the Case of Simultaneous Attacks”, *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), 2006, pp. 1-33.

[87] Hui, K.L., and Png, I. P. L. “Piracy and the Legitimate Demand for Recorded Music”, *Contributions to Economic Analysis & Policy* (2:1), 2003.

[88] Janczewski, L. J., and Colarik, A. M. “Managerial Guide for Handling Cyber-Terrorism and Information Warfare”, *Idea Group Publishing*, 2005.

[89] Jarrell, G., and Peltzman, S. “The Impact of Product Recalls on the Wealth of Sellers”, *The Journal of Political Economy* (93:1), 1985, pp. 512-536.

[90] Jordan, T., and Taylor, P. “A Sociology of Hackers”, *Sociological Review* (46:4), 1998, pp. 757-780.

[91] Kesan, J. P., Majuca, R. P., and Yurcik, W. J. “The Economic Case for Cyberinsurance”, *Securing Privacy in the Internet Age, Stanford University Press*, 2005.

[92] Kunii, A. “Corporate Risk and Information Security”, *Institute for International Policy Studies (IIPS), IIPS Policy Paper 269E*, Mar. 2001.

[93] Kunreuther, H., and Heal, G. “Interdependent Security”, *Journal of Risk and Uncertainty* (26:2-3), Mar. 2003, pp. 231-249.

[94] Lakhani, K. R., and Wolf, R. G.. “Why Hackers Do What They Do: Understanding Motivation and Effort in Free/Open Source Software Projects”, *In Perspectives on Free and Open Source Software*, 2005.

[95] Larsen, A. “Global security survey: Virus attack”, *InformationWeek.Com.*, 1999.

[96] Laudon, K. C., and Laudon, J. P. “Essentials of Management Information Systems : Managing the Digital Firm (6th Edition)”, *Upper Saddle River, NJ: Prentice Hall*, 2005.

[97] Leeson, P. T., and Coyne, C. J. “The Economics of Computer Hacking”.

[98] Lerner, J., and Tirole, J. “Some Simple Economics of Open Source”, *Journal of Industrial Economics* (50:2), 2002, pp. 197-234.

[99] Levy, S. “Hackers: Heroes of the Computer Revolution”, *Harmondsworth, UK: Penguin*, 1984.

[100] Loch, K. D., Carr, H. H., and Warkentin, M. E. “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding”, *MIS Quarterly* (17:2), 1992, pp. 173-186.

[101] Mackinlay, A. R. “Event Studies in Economics and Finance”, *Journal of Economic Literature* (35:1), Mar. 1997, pp. 13-39.

[102] Majuca, R. P., Yurcik, W., and Kesan, J. P. “The Evolution of Cyberinsurance”, *Cryptography and Security, Computers and Society*, Jan. 2006.

[103] Mark, J. E., and Tu, C. C. “An Event Study Analysis of Mall Renovation”, *Journal of Shopping Center Research* (12:2), 2005.

[104] Mears, J. “Is Security Ripe for Outsourcing?”, *Network World* (21:34), 2004, pp. 1-80.

[105] Michalowski, R. J., and Pfuhl, E. H. “Technology, Property, and Law - The Case of Computer Crime”, *Crime Law and Social Change* (15), 1991, pp. 255-275.

[106] Mulhall, T. “Where Have All the Hackers Gone? Part 3 - Motivation and Deterrence”, *Computers & Security* (16), 1997, pp. 291-297.

[107] Muralidhar, K., Batra, D., and Kirs, P. “Accessibility, Security, and Accuracy in

Statistical Databases: The Case for the Multiplicative Fixed Data Perturbation Approach", *Management Science* (41:9), Sep. 1995, pp. 1549-1564.

[108] Neumayer, E. "Socioeconomic Factors and Suicide Rates at Large Unit Aggregate Levels: a Comment", *Urban Studies* (40), 2003, pp. 2769–2776.

[109] Niederman, F., Brancheau, J. C., and Wetherbe, J. C. "Information Systems Management Issues for the 1990s", *MIS Quarterly* (17:4), 1991, pp. 475-500.

[110] NIST (National Institute of Standards and Technology). "An Introduction to Computer Security: The NIST Handbook", *Special Publication 800-12*, 1995.

[111] Nizovtsev, D., and Thursby, M. "Economic Analysis of Incentives to Disclose Software Vulnerabilities", *Working Paper*, 2005.

[112] Novak, T. P., and Hoffman, D. L. "Measuring the Flow Experience among Web Users", *Paper Presented at Interval Research Corporation*, 1997.

[113] Ozment, A. "Bug Auctions: Vulnerability Markets Reconsidered", *Workshop on Economics and Information Security, Minneapolis, USA*, May 2004.

[114] Parker, D. "Fighting Computer Crime: A New Framework for Protecting Information", *New York: John Wiley & Sons, Inc.*, 1998.

[115] Patell, J.M. "Corporate Forecasts of Earnings Per Share and Stock Price Behavior: Empirical Tests", *Journal of Accounting Research* (14:2), 1976, pp. 246-276.

[116] Peter, K. "Cyber-risk Assessors Chasing $2B market", *Philadelphia Business Journal* (20:50), 2002, pp. 4.

[117] Pfleeger, C. "Security in Computing", *Prentice Hall, Upper Saddle River, NJ: Prentice Hall*, 1997.

[118] Png, I. P. L., Tang, C. Q., and Wang, Q. H. "Hackers, Users, Information Security: Welfare Analysis", *27th ICIS, Milwaukee*, 2006.

[119] Pond, W. "Do Security Holes Demand Full Disclosure?", *ZDNet*, Aug. 2000.

[120] Post, J. "The Dangerous Information System Insider: Psychological Perspectives", 1996.

[121] Pouget, F., and Dacier, M. "Honeypot-based Forensics", *In AusCERT Asia Pacific Information Technolgoy Security Conference 2004* (AusCERT 2004), 2004.

[122] Pouget, F., Dacier, M., and Pham, V. H. “Understanding Threats: a Prerequisite to Enhance Survivability of Computing Systems”, *Proceedings of the International Infrastructure Survivability Workshop 2004, Lisbon, Portugal*, Dec. 2004.

[123] Power, R. “CSI/FBI Computer Crime and Security Survey”, *Computer Security Issues and Trends* (8:1), Jan. 2002, pp. 1-22.

[124] Rees, J., Bandyopadhyay, S., and Spafford, E. H. “PFIRES: A Policy Framework for Information Security”, *Communications of the ACM* (46:7), 2003, pp. 101-116.

[125] Rescorla, E. “Is Finding Security Holes a Good Idea?”, *The Third Workshop on the Economics of Information Security* (WEIS 2004), 2004.

[126] Rogers, M. “Psychology of Hackers: Steps Toward a New Taxonomy”, *Hacker Sitings and News*, 1999.

[127] Rohlfs, J. “A Theory of Interdependent Demand for a Communications Service”, *Bell Journal of Economics* (5:1), 1974, pp. 16-37.

[128] SANS Institute, “Glossary of Terms Used in Security and Intrusion Detection”, Available at http://www.sans.org/resources/glossary.php (last visited: Jul. 2006).

[129] Schechter, S. E. “Computer Security Strength & Risk: A Quantitative Approach” (PhD Thesis), *Harvard University, Cambridge, Massachusetts*, May 2004.

[130] Schechter, S. E. “Toward econometric models of the security risk from remote attacks”, *Security & Privacy Magazine, IEEE, MIT, MA, USA*, 2004, pp. 40-44.

[131] Schechter, S., and Smith, M. D. “Access for Sale: A New Class of Worm”, *WORM’03, Washington, DC, USA*, Oct. 2003.

[132] Schell, B. H., and Dodge, J. L. “The Hacking of America: Who’s Doing It, Why, and How”, *Quorum Books*, 2002.

[133] Schifreen, R. “What Motivates a Hacker?”, *Network Security, Oxford: Elsevier Science*, 1994, pp. 17-19.

[134] Schneier, B. “Applied Cryptography (2nd ed.)”, *Wiley, New York*, 1996.

[135] Schneier, B. “The Hackers are Coming!”, *Utility Automation & Engineering T&D*, Dec. 2005, Available at http://www.schneier.com/essay-097.html (last visited: Jul. 2006).

[136] Schwert, and William, G. “Using Financial Data to Measure the Effects of Regulation”, *Journal of Law & Economics* (24:1), Apr. 1981, pp. 121-158.

[137] Shapiro, C., and Varian, H. “Information Rules: A Strategic Guide to the Network Economy”, *Harvard Business School Press, Boston, Massachusetts*, 1999.

[138] Simmons, G. “Cryptanalysis and Protocol Failures”, *Communications of the ACM* (37:11), Nov. 1994, pp. 56–64.

[139] Spitzner, L. “Honeypots: Tracking Hackers”, *Addison-Wesley,* 2003.

[140] Sterling, B. “The Hacker Crackdown: Law and Disorder on the Electronic Frontier”, *Toronto: Bantam Books,* 1992.

[141] Straub, D. W. “Effective IS Security: An Empirical Study”, *Inf. Syst. Res.* (1:3), 1990, pp. 255-276.

[142] Straub, D. W., and Welke, R. J. “Coping with Systems Risk: Security Planning Models for Management Decision Making”, *MIS Quarterly* (23:4), 1998, pp. 441-469.

[143] Studenmund, A. H. “Using Econometrics: A Practical Guide (4th edition)”, *Addison Wesley,* 2001.

[144] Subramani, M., and Walden, E. “The Impact of E-Commerce Announcements on the Market Value of Firms”, *Information Systems Research* (12:2), 2001, pp.151.

[145] Symantec Inc. “Symantec’s Internet Security Threat Report”, Volume VI, Sep. 2004.

[146] Taylor, P. “Hackers: The Hawks and the Doves - Enemies & Friends” (Unfinished Manuscript), *In Rogers, M. “Psychological Theories of Crime and ‘Hacking’”*, 1999.

[147] Taylor, P. A. “Hackers: Crime in the Digital Sublime”, *London: Routledge*, 1999.

[148] Telang, R., and Wattal, S. “Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - An Empirical Investigation”, *The Fourth Workshop on the Economics of Information Security* (WEIS 2005), Feb. 2005.

[149] Turgeman-Goldschmidt, O. “Hackers’ Accounts: Hacking as a Social Entertainment”, *Social Science Computer Review* (23:1), 2005, pp. 8-23.

[150] U.S. Constitution, preamble.

[151] Vogel, T. A. “Dealing With Cyber Attacks on Network Security”, *48 PRAC. LAW, 36*, Apr. 2002.

[152] Voiskounsky A. E., and Smyslova, O. V. “Flow-Based Model of Computer Hackers’ Motivation”, *CyberPsychology & Behavior* (6:2), Apr. 2003, pp. 171 -180.

[153] Wattal, S., and Telang, R. “Effect of Vulnerability Disclosures on Market Value of Software Vendors - An Event Study Analysis”, *Carnegie Mellon University, Working Paper,* Sep. 2004.

[154] Westin, A. F. “Harris-Equifax Consumer Privacy Survey 1991”, *Equifax*, 1991.

[155] Whitman, M. E. “Enemy at the gate: Threats to information security”, *Communications of the ACM* (46:8), Aug. 2003, pp. 91–95.

[156] Whitman, M. E., and Mattord, H. J. “Principles of Information Security”, *Thomson Course Technology,* 2003.

[157] Willemson, J. “On the Gordon & Loeb Model for Information Security Investment”, *The Fifth Workshop on the Economics of Information Security* (WEIS 2006), 2006.

[158] Wiseman, S. “A Secure Capability Computer System”, *Proceedings of the IEEE Symposium on Security and Privacy: IEEE, Computer Society Press, Los Alamitos, California*, 1986, pp. 86–94.

Appendix

A: List of Countries' Abbreviation

Abbreviation	Full Name	Abbreviation	Full Name
AU	Australia	**BR**	Brazil
CA	Canada	**CN**	China
DE	Germany	**ES**	Spain
FR	France	**GB**	United Kingdom
IT	Italy	**JP**	Japan
KR	Korea	**NL**	Netherlands
PL	Poland	**SE**	Sweden
TW	Taiwan	**US**	United States

Table A: Abbreviations of Countries Investigated

B: The Detailed List of Events

Country	Event Date	Event Description	Source
CA	2005.01.06	9 months probation	National Post
	2005.11.17	Suspended from school for 30 days and is facing an expulsion hearing	The Toronto Star
	2006.01.17	3 years and 9 months in jail	Birmingham Post
CN	2005.03.21	a token fine of 1 RMB	http://www.315safe.com
	2005.03.23	Sentenced to 3 to 4 years in prison and fines	China Youth Daily
	2005.07.11	Arrested	BBC Monitoring Asia Pacific
	2005.07.12	Sentenced to 3 years in prison and a fine of 12,000 RMB	Wenhui Daily

	2005.10.19	Arrested	South China Morning Post
	2005.11.08	Arrested and accused	South China Morning Post
	2005.11.14	Arrested	Xinhua News Agency
	2005.11.15	Conviction of theft	China Daily
	2005.11.18	a maximum sentence of 3 years	Shanghai Daily
	2006.02.24	Arrested	http://www.yesky.com
	2006.04.10	Not punished just warning	South China Morning Post
	2006.04.15	Arrested and being sentenced	Xinhua News Agency
	2006.04.22	Sentenced to 1 year in jail	Xinhua News Agency
	2006.04.27	Arrested	Xinhua News Agency
	2006.05.12	Sentenced to 4 to 6 months in jail	Shanghai Evening Post
ES	2006.02.07	2 years in jail	M2 Presswire
	2006.04.08	up to 40 years in jail	Agence France Presse
UK	2005.01.30		The Independent
	2005.10.10	Found guilty and fined £400	Leicester Mercury
	2005.11.05	Sent to jail	The Northern Echo
	2005.12.30	up to 10 years in jail	The Daily Telegraph
	2006.01.17	Jailed for 3 years and 9 months	Birmingham Post
	2006.05.10	Extradited to and convicted in the US, up to 50 years in jail	Press Association Newswire
JP	2005.03.25	an 8-month prison sentence, but suspended for 3 years	BBC Monitoring Asia Pacific

	2005.04.14	Being investigated	http://www.chinanews.com.cn
	2005.11.10	Arrested	Kyodo News
NL	2005.10.10	Arrested and convicted	Xinhua News Agency
KR	2005.7.12	Arrested	http://www.sunm.net
	2006.05.21	Arrested	http://www.ccidnet.com
US	2005.01.29	18 months in prison	The Commercial Appeal
	2005.02.25	Suspended sentence	Northern Territory News/Sunday Territorian
	2005.03.14	6 months in jail	MIS New Zealand
	2005.10.14	a maximum penalty of 5 years imprisonment and a $250,000 fine	Vancouver Sun
	2005.10.22	Sentenced to 7 months	Rocky Mountain News
	2005.12.30	up to 10 years in jail	The Daily Telegraph
	2006.01.28	2 years in prison	Calgary Herald
	2006.04.13	2 years' probation and 200 hours of community service	The Courier-Mail
	2006.04.21	up to 10 years in federal prison	http://www.silicon.com
	2006.05.06	1 year of probation and ordered to pay $7,427 in restitution	The News Tribune
	2006.05.09	10 years in prison	CMP TechWeb
	2006.05.10	5 years in federal prison	Associated Press Newswires
	2006.05.11	3 years of imprisonment	Ukrainian National News Agency
	2006.05.16	4 years and 9 months in jail	The Gold Coast Bulletin
	2006.05.25	Prison time	CMP TechWeb

	2006.06.08	up to 30 years in prison and reimbursed his former employer	The Independent
	2006.06.09	20 years in prison and a $250,000 fine	VNUNet United Kingdom

Table B: The Detailed List of Events for the Eight Countries under Investigation