ABSTRACT

Title of Dissertation: The Value of Security Audits, Asymmetric Information and Market Impacts of Security Breaches

Lei Zhou, Doctor of Philosophy, 2004

Dissertation directed by: Professor Lawrence A. Gordon, Co-Chair/Co-Advisor
Professor Martin P. Loeb, Co-Chair/Co-Advisor
The Robert H. Smith School of Business

This dissertation includes two essays on the economic aspects of information security.

The first essay presents a principal-agent model for assessing the value of information security audits. The issue of information security investments is confounded by control problems arising from asymmetric information and conflicting managerial interests within the firm. By analyzing the impacts of asymmetric information and security audits, this study extends the literature in three ways. First, the degree of information asymmetry is formally measured, which allows one to study how different levels of information asymmetry affect information security investment decisions. Second, the intensity of an information security

audit is explicitly modeled, and the interactions between information asymmetry and security audits are examined. This analysis provides conditions under which the benefit from security audits increases with the degree of information asymmetry. Third, the current research provides an analytic model that helps to explain existing empirical findings (e.g., Gordon and Smith, 1992) concerning the relation between information asymmetry and the value of audits.

The second essay examines the economic costs of publicly announced information security breaches. Similar to Campbell et al. (2003), the current study applies the event study approach, but uses a larger sample and a more sophisticated market model (Fama and French, 1993). The results confirm those of Campbell et al. (2003) that security breaches involving confidential information cause significant market reactions and security breaches not involving confidential information only cause insignificant market reactions. Further investigations also suggest that the insignificance of market reactions to non-confidential events does not seem to vary with the nature of those events.

The Value of Security Audits, Asymmetric Information and Market Impacts of Security Breaches

by

Lei Zhou

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2004

Advisory Committee:

Professor Lawrence A. Gordon, Co-Chair/Co-Advisor
Professor Martin P. Loeb, Co-Chair/Co-Advisor,
Senior Research Scholar William Lucyshyn (School of Public Affairs)
Assistant Professor Partha Sengupta
Professor Claude E. Walston (College of Information Studies)

ACKNOWLEDGEMENTS

The author deeply thanks Dr. Lawrence A. Gordon and Dr. Martin P. Loeb for their helps and advice on this dissertation. The author is truly fortunate to have closely worked with them. Special gratitude goes to Dr. Gordon for his continuous support during the author's study at Maryland.

The author also thanks William Lucyshyn for his valuable comments and suggestions on issues of information security. In addition, the author thanks Tashfeen Sohail for his meticulous reading of the entire document, which has led to a much improved final version. Nonetheless, the author is solely responsible for any errors or omissions associated with this document.

TABLE OF CONTENTS

Chapter 1

Introduction

With wide adoption of computers and network technologies in organizations' information infrastructures, the threat from financial losses due to cyber intrusions and/or information security breaches also increases. According to the 2003 CSI/FBI Computer Crime and Security Survey, 75% of respondents had experienced financial losses related to security breaches. A total of $202 million worth of losses were reported by those organizations willing to provide an estimate of such losses (Richardson 2003). The actual social financial loss is considered to be even higher. A recent study by Campbell, Gordon, Loeb and Zhou (2003) captures indirect as well as direct costs of information security breaches by investigating the stock market reaction to the disclosure of such breaches. The evidence indicates a significant negative stock market reaction, when the information breached is of a confidential nature. Hence, protecting information assets from security breaches has become crucial for organizations.

This dissertation investigates two closely related, yet separate topics on economics of information security. The first part provides a theoretical model on the value of information security audits, especially, the effects of asymmetric

information during the security investment process are explicitly analyzed. The second part empirically examines the economic impacts of public announcements of information security breach incidents.

1.1 Background on Asymmetric Information and Security Investments

Along with the emphasis of information technologies, the expenditures by organizations in information security have increased significantly. Consequently, organizations have begun to realize the importance of rational information security investments. The objective of information security investments is not to obtain perfect security, but to protect the information system only to the extent that organizations receive the greatest net benefits from such protections. Some recent research has been done in this regard (e.g., Gordon and Loeb 2001, 2002). These studies, when considering the optimal amount to invest in information security, ignore the agency problem within organizations. They implicitly assume there's no information asymmetry between different levels of management, i.e., the Chief Executive Officer (CEO) and the Chief Information Security Officer (CISO) share the same knowledge not only about the security of information systems but the productivity of these investments as well. However, information asymmetry is a widespread phenomenon in reality. When interest conflict exists between different levels of management, information asymmetry may distort the top management's decisions. As a result, organizations are conducting various information security audits, believing they could help to reduce the negative effects caused by information asymmetry. Nonetheless, little, if any, research has

been dedicated to address the impacts of asymmetric information and security audits on security investment decisions.

The primary objective of the first part of this dissertation is to show that an information security audit provides value to an organization by reducing information asymmetry between the CEO and the CISO. More specifically, an analytical model, based on a principal-agent framework, is used to capture the characteristics of the problem. The model shows that when there exists information asymmetry, CISOs may receive information rents, and CEOs' investment decision rules tend to deviate from those when there is no information asymmetry. This deviation leads to an increase in CEOs' total expected costs. Security audits act to improve CEOs' understanding of the system, hence reduce the effects of the information asymmetry between CEOs and CISOs. As a result, CEOs' investment decision rules become closer to the optimal (full information) rules. Another interesting result from the model is that the value of an information security audit also depends on the information environment. As the information asymmetry between CEOs and CISOs increases, the value of an information security audit also increases.

1.1.1 Security Audits and Postaudits of Security Investments

Many consulting firms, specializing in either technology or accounting, provide various security services. These services are conducted under different names, like "security tests", "system integration" and "vulnerability check". One key feature of these services is an information security audit. The purpose of a security audit is to evaluate the internal controls in information systems. It helps to

detect systems' errors, regardless of the causes, either technological or human. The actual scope of security audits may include analyzing network infrastructures, reviewing implementation of systems' controls, verifying administrative controls, and identifying the vulnerability of the systems. The results from a security audit can be used to help management better understand pre-conditions of information systems before security investments and hence allocate economic resources more efficiently.

Another type of audit, postaudits, are also commonplace in practice. In a postaudit, the actual benefits from an investment are examined and compared with the estimates made before the investment. Research has shown that an appropriate match between the sophistication of a postaudit and the level of information asymmetry is associated with better firm performances on the stock market (e.g., Gordon and Smith, 1992). For information security investments, a postaudit can also be conducted to evaluate the actual cost savings from the investments. Besides the different emphases of information security audits and postaudits of information security investments, the two type of audits also differ in the time when they are conducted. Information security audits can be conducted both before and after information security investments, while postaudits of information security investments can only be conducted after the results from the security investments have been realized. The current study will focus on security audits and leave postaudits of security investments for future research.

1.2 Background on Impacts of Security Breaches

The purpose of information security is to protect organizations' information assets, to ensure the confidentiality, integrity and accessibility of information systems. While the actual protection measures are mostly technological in nature, the question of allocating limited economic resources in various security procedures is more of an economic issue. In recent years, there have been a number of theoretical studies applying economic analyses in the issues of information security investments. For instance, Gordon and Loeb (2001, 2002) suggest that, contrary to conventional wisdoms, it may not always be optimal to invest the most money in information system with the highest vulnerability. Only after thorough considerations of the potential financial loss, the vulnerability of the system and costs of protecting the information, a cost-benefit efficient security investment decision can be made.

In order to make appropriate security investment decisions, the financial losses related to security breaches have to be better understood. There is much anecdotal evidence regarding the economic impacts of security breaches. While some view information breaches as a serious threat to the economy, others suggest that they might be just a daily cost of doing business in the new information age. In the existing literature, most of the research investigating the costs of security breaches is survey-based. These studies show that majority of the organizations have experienced information security breaches during the last decade and suffered significant financial losses. However, these surveys usually focus on the direct costs of information security breaches (such as loss of business due to denial-of-service attacks, or the costs of repairing the system after outbreaks of computer viruses). The indirect costs of security breaches, such as reputation

loss or decreased future sales are often ignored, making it difficult to present a complete picture of the impacts of security breaches. There are a few exceptions employing another approach, the event-study method (e.g., Campbell et al., 2003, Garg, Curtis and Halper, 2003, Ettredge and Richardson, 2002 and Cavusoglu, Birendra and Raghunathan, 2002). These studies examine the market reactions to information security breaches. The market reactions can reflect the changes of investors' expectations of future cash flows due to security breaches, thus capture both direct and indirect costs of information security breaches.

The second part of this dissertation is an extension study following Campbell et al. (2003). By expanding the scope of the event search, the current research presents a larger sample. To better capture the market expectations, this study also adopts the Fama and French (1993) three-factor model about returns on common stocks. New hypotheses are developed and tested, the results provide both enhanced empirical support to the conclusions of Campbell et al. (2003) and new insights on the economic impacts of information breaches.

1.3 Literature Review

1.3.1 Information Asymmetry and Principal-Agent Model

Information asymmetry and interest conflicts between the different parties within organizations have long been recognized by both the business world and academic researchers. As Harris, Kriebel and Raviv (1982) state, "... in most firms, various tasks are performed or managed by different individuals each of whom has special information or expertise concerning his particular sphere of activity. Usually this information is not available to other individuals within the firm including

the top management." They further point out that "individuals with private information also have interests which may diverge from those of the firm and therefore may find it disadvantageous to reveal their privileged information freely to top management." The impact of these two factors on top management's decisions has been one of the central topics in management accounting research.

When the action of division managers (the agent) cannot be observed by the headquarters (the principal), moral hazard problems arise. Holmstrom (1979) is among the first to characterize this phenomenon using a theoretical model, analyzing the interaction between a risk-neutral principal and a risk-averse agent. Holmstrom (1979) shows that when the agent's action is unobservable, the principal may have to deviate from the optimal risk sharing rules when designing the contract. The risk-averse agent is exposed to a certain amount of risk so that he would be motivated to work towards the benefits of the firm.

Besides the agent's hidden action, another form of information asymmetry between the principal and the agent, hidden information, is also a widespread phenomenon.[1] When working on his delegated duties, the agent may acquire private information on the productivity of the technology adopted or the underlying state of the situation. Since this information is not available to the principal, the agent may use it to pursue his personal utility maximization instead of maximizing the firm's profit. Including both hidden action and hidden information, Harris, Kriebel and Raviv (1982) study the impacts of asymmetric information and interest conflict on intrafirm resource allocation decisions.

Using a similar setup with Harris, Kriebel and Raviv (1982) but focusing on

[1]Based on the nature of principle-agent problems, Arrow (1985) first divides information asymmetry into two categories: hidden action and hidden information.

only hidden information, Antle and Eppen (1985) study the rationing of capital investments. Their analyses suggest that if the agent possesses private information about the return of investments, the principal will allocate the agent excess resources (organizational slack). In some situations the optimal allocation policy involves a hurdle rate greater than the cost of capital. The excess resources are actually the information rent the principal pays to motivate the agent to report truthfully. Neither the information rent nor the investment decisions are ex post efficient; the optimal policy is just a trade-off between the two inefficiencies. The studies in the literature agree that, when the principal and agent have different goals, the existence of information asymmetry brings negative effects on the firm's performance and causes distortion of headquarter's investment decisions, as pointed out in Baiman (1990) "..., as a result of agency problems, often the best that the principal can do is to distort production, risk-sharing and wealth allocation from first best."

To reduce such negative effects caused by information asymmetry, organizations engage in various monitoring/auditing activities. The effects of different monitoring/auditing strategies raises interesting research questions in accounting. Ng and Stoeckenius (1979) show that, in the case of hidden action, when the principal has to depend on the agent to report the outcomes of the agent's action, it becomes nearly impossible for the principal to motivate the agent. An effort-averse agent can always choose a reporting strategy that conveys no information on his effort, thus never have to work. An audit of the agent's report has value to the principal because it can induce truthful reporting while providing incentives to the agent to work. Baron and Besanko (1984) also examine the demand of audits under a regulator *versus* firm framework. In their model, the

firm has private information about its cost, which in turn affects the regulator's price decision. The regulator may verify the firm's report on cost through an audit. They derive the optimal auditing strategy and prove that it improves the social welfare.

While in much research (e.g., Baron and Besanko, 1984), the principal is assumed either to always conduct an audit, or to conduct an audit with a probability, Dye (1986) deals with the optimality of lower-tailed audits. Lower-tailed audits differ from the two types of audits mentioned above. As the name implies, lower-tailed audits refer to deterministic audit policies that an audit always happens when the outcome is lower than a threshold and never happens when the outcome is higher than such threshold. Dye (1986) points out that in some situations, when the principal can choose to audit on the agent's hidden action, a low-tailed audit is optimal.

Kim and Suh (1992) further extend the literature by allowing the principal to determine the level of audit investments. They assume that the principal can choose to invest in the monitoring technology which reveals information on the agent's hidden action. The optimal precision of the monitoring information is endogenously determined in their model. They find that under a concave monitoring technology, there exists interior optimal auditing strategy, that is, it is not always optimal for the principal to conduct the audit, the audit will happen randomly with a probability less than one. The principal tends to invest more in monitoring when the outcome is worse. However, under a linear monitoring technology, the principal will choose a deterministic auditing strategy, which is very similar to the lower-tailed auditing derived by Baiman and Demski (1980) and Dye (1986).

Harris and Raviv (1996) is more focused on the effects of auditing during the capital budgeting process. Similar to Antle and Eppen (1985), they also assume the agent has better information on the productivity of investment than the principal. Unlike Antle and Eppen (1985), Harris and Raviv (1996) incorporate a random audit in their capital budgeting process, assuming that the audit can perfectly reveal the agent's private information to the principle. Their results show that without an audit, the principle has to deviate from the optimal (NPV maximizing) investment decisions in order to take advantage of the agent's private information. More specifically, the principal tends to overinvest in the project with lower productivity and underinvest in the project with higher productivity. A pre-committed audit policy can effectively reduce the costs resulted from motivating the agent.

A majority of the studies on the value of auditing/monitoring are based on the assumption that the principal can pre-commit to some auditing policy. Since most of the time the agent is induced to comply with the contract, it might be ex post inefficient for the principal to conduct an audit. Khalil (1997) addresses the issues on auditing without commitment. He compares the case where the principal can pre-commit to an audit with the case where the principal cannot pre-commit, but can make an audit decision after the outcomes are realized. He finds that when the principal can pre-commit, he will design the contract so that the agent is unlikely to deviate from the contract. On the contrary, when the principal cannot pre-commit, he will design the contract such that he tends to audit more frequently. This suggests that when the threats of auditing are credible, the principal relies more on the contract to motivate the agent, while when the threats are not credible, the principal relies more on the audit

to motivate the agent.

Beside the analytical studies mentioned above, a lot of empirical research has also been done in the field of the information asymmetry and audits (e.g., Guillver, 1987, Myers, Gordon and Hamer, 1991, Gordon and Smith, 1992). These empirical studies support the argument that audits/postaudits can add value to the firms, e.g., the proper use of auditing procedures is positively related to the firm's long-term performance.

Both the analytical and empirical studies agree that the information asymmetry has negative effects on organizations' decision processes, and by adopting certain auditing procedures these negative effects can be reduced. When discussing the effects of auditing under information asymmetry, most studies typically assume that once an audit is conducted it reveals all the information the agent withholds from the principal, even though the audit may only happen with a certain probability. The information asymmetry between the principal and the agent is generally deemed as a fixed background, in other words, the degree of information asymmetry is rarely mentioned. One exception is Gordon and Smith (1992). In their empirical tests they identify explicit proxies for both information asymmetry and the sophistication of postauditing procedures. They show that level of information asymmetry is an imperative factor in the application of postauditing. Only a proper match between the level of information asymmetry and the level of postauditing is associated with better performance of firms on the stock market.

The model provided by the current study extends the literature in three ways. First, the degree of information asymmetry is explicitly modeled. Like in previous analytical work, the agent is assumed to possess private information

about the investment environment. Moreover, at the meantime, the principal can also observe an imperfect signal of the information the agent possesses. The difference between the signal the principal observes and the more precise information the agent possesses is explicitly described and used to measure the degree of information asymmetry between the principal and the agent. This measure enables the examination of how the principal's investment decisions vary with the degree of the information asymmetry.

Second, security audits are assumed to be common procedures in security investment processes, but they can only partially reveal the agent's private information to the principal. Thus the effects of audits on the principal's decisions and the interaction between the magnitude of information asymmetry and the accuracy of the audits can be formally examined.

And finally, the current model also provides a theoretical explanation to the empirical results reported by Gordon and Smith (1992).

1.3.2 Impacts of Security Breaches

While today's business world enjoys the benefits of information technologies, the occurrences of information security breaches have become ubiquitous and pose a serious question to both practitioners and researchers. Some argue that security intrusions have caused severe financial loss to the breached firms, others view the security breaches only as a normal cost of business. While there have been numerous anecdotal reports from the media supporting both arguments, whether information security breaches have significant economic impacts on the affected firms remains an empirical question.

Many survey studies conducted in recent years (e.g., Yankee Group, 2000,

Computer Economics Institute, 2002, Riverhad Networks, 2002, KPMG, 2002 and CSI/FBI survey, 2002, 2003) have documented the prevalence and magnitude of information security breaches. Among these, Yankee Group (2000) suggested that the denial-of-service attacks in February 2000 alone have caused financial losses that totaled $1.2 billion. Based on the responses from 538 U.S. firms, CSI/FBI survey (2002) found that in 2002, about 90% of the respondents had experienced security breaches and on average, each security breach accident costed $1.95 million. However, survey studies derive the results mostly from the estimations provided by the responding organizations, which tend to include only the direct costs. Moreover, the survey questionnaires are often of a descriptive nature, which also limits the possibility of statistically evaluating the economic impacts of information security breaches.

In contrast, the event-study approach examines the stock market reactions to events under questions. The change of the stock price due to an information security breach announcement incorporates the market's perception of not only the short-term costs incurred at the time of the breach, but also long-term costs after the breach. A number of event studies regarding information security breaches have been conducted. Among these studies, Ettredge and Richardson (2002) investigated the impacts of February 2000's denial-of-service attack. Firms involved in e-commerce were divided into two groups, B2C (business to consumers) firms and B2B (business to business) firms. In their study, they found that during the test window around the denial-of-service attack, in comparison with the market, the stock prices of both B2C and B2B firms dropped significantly.

Using a market model, Cavusoglu et al. (2002) and Garg et al. (2003) both

examined information security breaches' impacts on the stock prices of breached firms. Cavusoglu et al. (2002) showed that on average, small firms and firms depending heavily on the Internet were associated with greater negative market reactions to announced security breaches. They also detected a significant information transfer effect, that is, the stock prices of Internet security firms increased significantly around the time when security breaches were announced. Excluding all the computer virus events, Garg et al. (2003) presented similar results regarding the price reactions of breached firms, and confirmed the information transfer effect.

Campbell et al. (2003) employed the CAPM model and studied the economic cost of publicly announced information security breaches. Besides the standard ordinary least square (OLS) regression, they also applied the seemingly unrelated regression (SUR) method to control the heteroskedasticity and event clustering problems. Both methodologies showed that announcements of information breach incidents only induced marginal negative market reactions. However, further investigations revealed that the significance of market reactions depended on the nature of the breaches. For information breaches involving confidentiality (i.e., unauthorized access to proprietary information such as credit card numbers), the affected firms' stocks had statistically significant negative price reactions, while for those breaches involving only non-confidential information, the market reactions were not statistically significant.

The results of Campbell et al. (2003) provide insights on the decisions of information security investments. Given that the breaches involving confidential information tend to cause more severe economic consequences, organizations should put more efforts safeguarding their confidential information assets, if all

other things are equal. However, there are still some unsolved concerns on the market's reaction to information security breaches. Campbell et al. (2003) used CAPM to measure the abnormal returns from the market. A lot of studies (e.g., Fama and French, 1992, 1993, 1996) on capital market have suggested that a single factor model like CAPM is not adequate to fully capture the multi-dimension risks of the stock market. The second concern arises from the fact that Campbell et al. (2003) did not differentiate between virus-based events and non-virus-based events. As suggested by prior research (e.g. Garg et al., 2003), computer viruses are trivial in nature, thus inclusion of virus-based information security breaches may confound the results of event studies. So it would be interesting to see if the results of Campbell et al. (2003) are sensitive to further partition of the non-confidential events based on whether they were caused by computer virus. The last concern is about the limited sample size in Campbell et al. (2003). In econometrics, small sample sizes always lead to criticisms that the results may not be representative. A larger and more comprehensive sample would help to verify the validity of their conclusions.

The current study addresses the above concerns. First, this study extends both the news sources and time period in the event search, thus increasing the sample size; second, a more sophisticated model (Fama and French 1993 three-factor model) is adopted to assess the market reactions; and last, the non-confidential security breach events are further partitioned based on whether they are computer virus based, and the market reactions of each group are examined.

1.4 Plan of Chapters

The rest of this dissertation is organized as follows. Chapter 2 presents an analytic model on asymmetric information and information security audits. The results and insights from the model are also discussed in Chapter 2. Chapter 3 is dedicated to the empirical study on the impacts of information security breaches. Chapter 4 provides some concluding remarks of this dissertation. The notations and symbols used in the analytical model are listed in Chapter 5. The detailed mathematical proofs for the model are provided in the Appendix.

Chapter 2

Model on the Value of Information Security Audits

2.1 Model Setup

CISOs generally have better and more timely information about the security of their firms' computer systems than do the firms' CEOs. The CEOs have the ultimate decision-making authority for allocating resources, improving the information systems' security, and yet rely on information provided by the CISOs. The CEOs are more concerned about the efficiency of security investments, but the CISOs focus on the level of system security. This leads to a typical principal agent setup in economics literature (e.g., Holmstrom 1979), where the CEOs behave as the principal and the CISOs as the agent.

Assume if a security breach were to happen, the organization would incur loss L.[1] Denote $P(\alpha, x)$ as the chance that a security breach of the information system will happen. x is the amount of information security expenditures, and

[1]For simplicity, the model only considers the scenario where there is only one possible breach, this setup follows directly from Gordon and Loeb (2001).

α represents the state of information system. $P(\alpha, x)$ satisfies the following conditions:

$$\begin{aligned} P_x(\alpha, x) &= \frac{\partial P(\alpha, x)}{\partial x} < 0, \\ P_{xx}(\alpha, x) &= \frac{\partial^2 P(\alpha, x)}{\partial x^2} > 0, \\ \lim_{x \to \infty} P(\alpha, x) &= 0, \end{aligned}$$

where $x \geq 0$.

As the amount spent in information security increases, the probability of a security breach decreases, i.e., the expected cost saving from avoiding a security breach increases. However, such cost saving increases at a decreasing rate as the investment increases. As the security investment approaches infinity, the probability of a security breach approaches zero.

The different values of α will impact the effects of information security expenditures. For simplicity, assume α can only take two possible values, i.e., $\alpha = \{\alpha_H, \alpha_L\}$. More specifically, let

$$\alpha = \begin{cases} \alpha_H & \text{w.p. } P_H, \\ \alpha_L & \text{w.p. } P_L, \end{cases}$$

where P_H is the probability that $\alpha = \alpha_H$, $P_H + P_L = 1$ and $\alpha_H > \alpha_L$. Also assume that

$$\begin{aligned} P(\alpha_H, x) &> P(\alpha_L, x), \\ P_x(\alpha_H, x) &< P_x(\alpha_L, x). \end{aligned}$$

Note that the meaning of α is two-fold. First, α represents the vulnerability of the information system. A higher α implies a higher chance of a security breach, thus, α_H reflects a high vulnerable system and a worse situation for the principal.

Second, α also reflects the productivity of information security investments. The marginal benefit of security investments is greater under α_H, hence α_H means higher productivity of security investments.

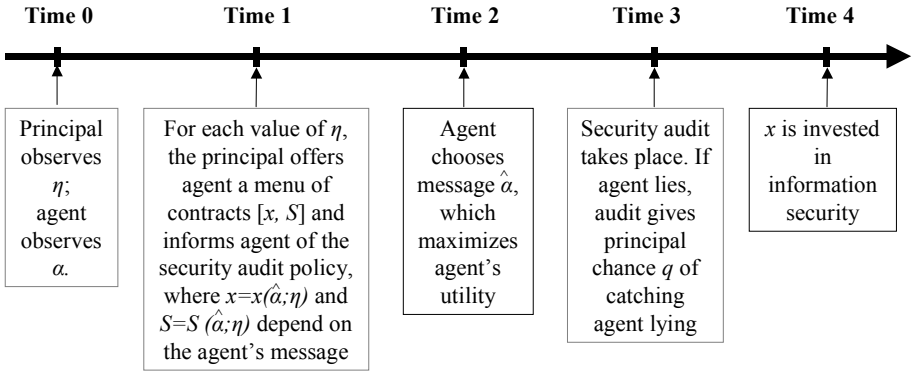
Since the principal does not work directly on information systems, she has less detailed knowledge than the agent. More specifically, the agent can directly observe the true value of α, while the principal can only observe η, a signal of α, where $\eta = \{\alpha_H, \alpha_L\}$. Let the chance that principal knows the true value of α by observing η be ξ $(0 \leq \xi \leq 1)$, formally stated as:

$$\begin{cases} P(\eta = \alpha_H | \alpha = \alpha_H) = \xi, \\ P(\eta = \alpha_L | \alpha = \alpha_L) = \xi. \end{cases}$$

Note that if η is negatively correlated with α, i.e., $0 \leq \xi < \frac{1}{2}$, the principal can always interpret signal η reversely. Thus, without loss of generality, the model only discusses the case where $\frac{1}{2} \leq \xi \leq 1$.

The magnitude of ξ measures the information asymmetry between the principal and the agent. When $\xi = \frac{1}{2}$, η does not provide any useful information about α, the signal observed by the principal is independent of the value of the true state, the information asymmetry between principal and agent is the most severe. As ξ increases, signal η provides reflect information on α, that is, the information asymmetry decreases. When $\xi = 1$, η contains perfect information about α. In this case, the principal observes exactly the same signal as the agent does, hence there is no information asymmetry between the principal and the agent.

Figure 2.1 presents the timeline structure of the model. At time 0, the principal observes signal η while the agent observes the true state of α. The principal then forms a belief about the true state of α given her observation.



Notations:

1. ***α = productivity of information security investment***
2. ***$\hat{\alpha}$ = agent's message, a report of the productivity parameter α observed by the agent***
3. ***η = signal of α observed by the principal***
4. ***x = information security investment level***
5. ***S = salary for agent***

Figure 2.1: Timeline

At time 1, since the principal cannot observe the true state on her own, in order to minimize her total costs, she would utilize the agent's information by having the agent report the α he observed. The principal designs a menu of contracts based on her belief to minimize her total expected expenditures. The contracts include the security investment amount x and the agent's salary $S \geq 0$, where the amounts of both depend on the agent's report $\hat{\alpha}$. Meanwhile, the principal also informs the agent of the security audit policy, which determines the intensity of security audits.

At time 2, the agent selects the message $\hat{\alpha}$ that he reports to the principal. Based on the contracts offered by the principal, the agent will choose the $\hat{\alpha}$ that leads to a contract maximizing his own utility.

At time 3, the principal conducts the security audit as she committed. If the principal were to conduct a complete system security check, the agent would be caught when he's lying. Let q be the chance that a security audit would discover the truth if the agent lied. Once found lying, the agent will be removed immediately and end up with zero utility. q represents the intensity of information security audits.

At time 4, information security investment takes place. The agent invests x in security.

At time 5, the results from security investment x are realized. The principal may choose to postaudit these results and determine how much have been saved by avoiding security breach.

The agent would also suffer from a security breach, since he may have to endure certain reputation loss in the marketplace, or have certain intrinsic disutility from having a breach, etc. Let βL be the agent's disutility should a security

breach happen. β measures the extent to which the agent suffers from security breaches, where $\beta \ll 1$. The expected disutility of the agent from a security breach can be written as $\beta P(\alpha, x) L$.[2]

During the process of information security investment, the principal is burdened with the cost of information security investments, thus she always tries to use such investments as efficiently as possible. However, the agent only cares about the resulting security level and wishes to get as much investment as possible. This causes an interest conflict between the principal and the agent.

The model will focus on the events happening from time 0 to time 4, the effects of postauditing will be left for future research.

2.2 Full Information Case

Before the discussions on the implications of information asymmetry, the full information case will be introduced first as a benchmark.

In the full information case, there exists no information asymmetry, that is, $\xi = 1$. The principal knows exactly what the agent knows. The principal decides the optimal investment level and the agent's salary to minimize her total expected costs, which is the sum of the expected loss from security breaches, the amount invested in information security and the agent's salary. Assuming the agent's reservation utility is zero, the principal's problem is:

$$\min_{x,S} P(\alpha, x) L + x + S,$$

[2]This is somewhat analogous to a feature of the model of Harris and Raviv (1996), in which a division manager's utility increases with the allocation of capital to the division.

subject to

$$S - \beta P(\alpha, x) L \geq 0.$$

When the true state is α_H, the first order conditions are:

$$(1+\beta) P_x(\alpha_H, x_H^*) L + 1 = 0, \tag{2.1}$$

$$S_H^* - \beta P(\alpha_H, x_H^*) L = 0; \tag{2.2}$$

when the true state is α_L, the first order conditions are:

$$(1+\beta) P_x(\alpha_L, x_L^*) L + 1 = 0, \tag{2.3}$$

$$S_L^* - \beta P(\alpha_L, x_L^*) L = 0, \tag{2.4}$$

where x_H^*, S_H^*, x_L^*, S_L^* are solutions to the above equations. Given $P_x(\alpha_H, x) < P_x(\alpha_L, x)$, it can be easily shown that

$$x_H^* > x_L^*,$$

the principal simply invests more in information security when the system is more vulnerable. The agent's expected utility is the reservation utility (zero) in both states.

2.3 Imperfect Information Case

2.3.1 Principal's Inference

When there exists information asymmetry, i.e., $\frac{1}{2} \leq \xi < 1$, the principal only observes an imperfect signal. However, she can formulate beliefs about the true state based on the observed signal η.

The joint distribution of α and η is:

	$\alpha = \alpha_H$	$\alpha = \alpha_L$
$\eta = \alpha_H$	ξP_H	$(1-\xi) P_L$
$\eta = \alpha_L$	$(1-\xi) P_H$	ξP_L

If the principal observes $\eta = \alpha_H$, she can infer, using Bayes' rule, that

$$\begin{aligned}
\Pr(\alpha = \alpha_H | \eta = \alpha_H) &= \frac{\Pr(\alpha = \alpha_H, \eta = \alpha_H)}{\Pr(\eta = \alpha_H)} \\
&= \frac{\Pr(\alpha = \alpha_H, \eta = \alpha_H)}{\Pr(\alpha = \alpha_H, \eta = \alpha_H) + \Pr(\alpha = \alpha_L, \eta = \alpha_H)} \\
&= \frac{\xi P_H}{\xi P_H + (1-\xi) P_L}.
\end{aligned}$$

Similarly, the principal can formulate the following conditional probabilities about the true states.

$$\begin{aligned}
\Pr(\alpha = \alpha_L | \eta = \alpha_H) &= \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}, \\
\Pr(\alpha = \alpha_H | \eta = \alpha_L) &= \frac{(1-\xi) P_H}{(1-\xi) P_H + \xi P_L}, \\
\Pr(\alpha = \alpha_L | \eta = \alpha_L) &= \frac{\xi P_L}{(1-\xi) P_H + \xi P_L}.
\end{aligned}$$

The marginal distribution of η is

$$\begin{aligned}
\Pr(\eta = \alpha_H) &= \xi P_H + (1-\xi) P_L, \\
\Pr(\eta = \alpha_L) &= (1-\xi) P_H + \xi P_L.
\end{aligned}$$

2.3.2 Minimizing Principal's Expected Costs

Based on her belief, the principal will design the contract to minimize her expected costs. Denote the principal's minimized expected costs as C_H when

$\eta = \alpha_H$ is observed, and C_L when $\eta = \alpha_L$ is observed. The ex ante expected costs of the principal before observing signal η are

$$C = \Pr(\eta = \alpha_H) C_H + \Pr(\eta = \alpha_L) C_L,$$

where $\Pr(\eta = \alpha_H) = \xi P_H + (1 - \xi) P_L$ is the probability that the principal observes $\eta = \alpha_H$, and $\Pr(\eta = \alpha_L) = (1 - \xi) P_H + \xi P_L$ is the probability that the principal observes $\eta = \alpha_L$.

By the revelation principal,[3] only the contracts inducing the agent to tell the truth need to be considered, that is, the principal will design the contract such that the agent is motivated to always tell the truth in his report. Figure 2.2 illustrates the agent's payoff under various scenarios. When the principal observes $\eta = \alpha_H$ and the agent reports $\hat{\alpha} = \alpha_H$, the agent will receive x_{HH} as the amount of security investment and S_{HH} as the agent's salary; when the principal observes $\eta = \alpha_H$ and the agent reports $\hat{\alpha} = \alpha_L$, the agent will receive x_{HL} and S_{HL}; when the principal observes $\eta = \alpha_L$ and the agent reports $\hat{\alpha} = \alpha_H$, the agent will receive x_{LH} and S_{LH}; when the principal observes $\eta = \alpha_L$ and the agent reports $\hat{\alpha} = \alpha_L$, the agent will receive x_{LL} and S_{LL}.

If the principal observes $\eta = \alpha_H$, she infers that the probability of α_H being the true state is $\Pr(\alpha = \alpha_H | \eta = \alpha_H)$, and the probability of α_L being the true state is $\Pr(\alpha = \alpha_L | \eta = \alpha_H)$. Hence, C_H can be formally expressed as:

$$C_H = \min_{x_{HH}, S_{HH}, x_{HL}, S_{HL}} \left\{ \frac{\xi P_H}{\xi P_H + (1 - \xi) P_L} \left[P(\alpha_H, x_{HH}) L + x_{HH} + S_{HH} \right] \right.$$
$$\left. + \frac{(1 - \xi) P_L}{\xi P_H + (1 - \xi) P_L} \left[P(\alpha_L, x_{HL}) L + x_{HL} + S_{HL} \right] \right\}$$

[3]For detailed derivation and discussion on the revelation principal, see Myerson (1979).

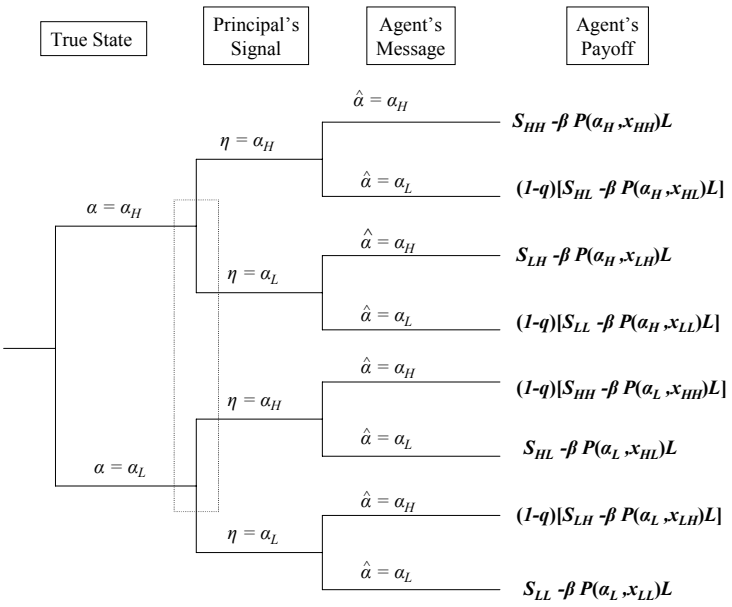


Figure 2.2: Agent's Payoff

subject to

$$S_{HH} - \beta P(\alpha_H, x_{HH}) L \geq 0, \tag{2.5}$$

$$S_{HL} - \beta P(\alpha_L, x_{HL}) L \geq 0, \tag{2.6}$$

$$S_{HH} - \beta P(\alpha_H, x_{HH}) L \geq (1-q)[S_{HL} - \beta P(\alpha_H, x_{HL}) L], \tag{2.7}$$

$$S_{HL} - \beta P(\alpha_L, x_{HL}) L \geq (1-q)[S_{HH} - \beta P(\alpha_L, x_{HH}) L]. \tag{2.8}$$

Constraints (2.5) and (2.6) make sure that the agent will get at least his reservation utility regardless the true state he observes. Constraint (2.7) guarantees that the agent's utility from telling the truth is greater than or equal to his utility from lying when he observes worse state ($\alpha = \alpha_H$). Constraint (2.8), following the same logic, guarantees the agent's utility from truth-telling is no less than his utility from lying when he observes the better state ($\alpha = \alpha_L$). The

last two constraints ensure that the agent can get as least as much utility when he tells the truth as he lies. In other words, the principle designs the contracts in a way that the agent never has incentives to lie in his report. In the rest of discussions, when the agent's report is mentioned, α will be used instead of $\hat{\alpha}$ since $\hat{\alpha}$ will always truthfully reflect the true state α.

Similarly, when the principal observes $\eta = \alpha_L$, the principal's problem becomes

$$C_L = \min_{x_{HH}, S_{HH}, x_{HL}, S_{HL}} \left\{ \frac{(1-\xi) P_H}{(1-\xi) P_H + \xi P_L} \left[P(\alpha_H, x_{LH}) L + x_{LH} + S_{LH} \right] \right.$$
$$\left. + \frac{\xi P_L}{(1-\xi) P_H + \xi P_L} \left[P(\alpha_L, x_{LL}) L + x_{LL} + S_{LL} \right] \right\}$$

subject to

$$S_{LH} - \beta P(\alpha_H, x_{LH}) L \geq 0, \tag{2.9}$$

$$S_{LL} - \beta P(\alpha_L, x_{LL}) L \geq 0, \tag{2.10}$$

$$S_{LH} - \beta P(\alpha_H, x_{LH}) L \geq (1-q) \left[S_{LL} - \beta P(\alpha_H, x_{LL}) L \right], \tag{2.11}$$

$$S_{LL} - \beta P(\alpha_L, x_{LL}) L \geq (1-q) \left[S_{LH} - \beta P(\alpha_L, x_{LH}) L \right]. \tag{2.12}$$

Let $\hat{x}_{HH}$, $\hat{S}_{HH}$, $\hat{x}_{HL}$, $\hat{S}_{HL}$ be the solutions to the optimization problem when $\eta = \alpha_H$, and $\hat{x}_{LH}$, $\hat{S}_{LH}$,$\hat{x}_{LL}$, $\hat{S}_{LL}$ be the solutions to the optimization problem when $\eta = \alpha_L$, the next section will discuss the features of these solutions.

2.4 Benefits of Security Audits

The following lemma give the characteristics of the constraints.[4]

[4]Detailed proofs of lemmas and propositions are provided in the appendix.

Lemma 1 *Constraints (2.8) and (2.12) bind; constraints (2.6) and (2.10) are redundant.*

Constraints (2.6) and (2.10) guarantee the agent get his reservation utility when he observes $\alpha = \alpha_L$, while constraints (2.8) and (2.12) induce the agent to report the state α_L truthfully. Since the principal is inclined to invest less under the state α_L, when the agent observed $\alpha = \alpha_L$, he has the incentive to send a false report so that he can get more investments. In order to make the agent tell the truth, the principal has to provide additional incentives to compensate the agent. As a result, the truth-telling constraint binds, and the agent will get a utility greater than the reservation utility when he observe $\alpha = \alpha_L$.

Lemma 2 *Constraints (2.5) and (2.9) bind; constraints (2.7) and (2.11) are redundant.*

When the agent observes $\alpha = \alpha_H$, he does not have incentives to lie unless the principal over-compensates the agent for telling $\alpha = \alpha_L$. However, since the principal will minimize her own expected costs, over-compensating would contradict her objective. Hence, when $\alpha = \alpha_H$ is observed by the agent, the truth telling constraint is redundant and reservation utility constraint binds.

Proposition 1 *Compared with the full information solutions, the imperfect information solutions have the following features, regardless of the principal's signal: when the agent reports $\alpha = \alpha_H$, the principal invests more than she does in the full information case and the agent receives less salary; when the agent reports $\alpha = \alpha_L$, the principal invests the exactly same amount as she does in the full information case and the agent receives more salary, i.e.,*

$$\hat{x}_{HH} > x_H^*, \text{ and } \hat{x}_{LH} > x_H^*; \tag{2.13}$$

$$\hat{x}_{HL} = x_L^*, \text{ and } \hat{x}_{LL} = x_L^*; \tag{2.14}$$

$$\hat{S}_{HH} < S_H^*, \text{ and } \hat{S}_{LH} < S_H^*; \tag{2.15}$$

$$\hat{S}_{HL} > S_L^*, \text{ and } \hat{S}_{LL} > S_L^*. \tag{2.16}$$

Intuitively, since the agent cannot benefit from reporting $\alpha = \alpha_L$ if he actually observes $\alpha = \alpha_H$. Thus, the principal tends to trust a report that $\alpha = \alpha_L$ and sticks to the optimal investment level. However, when the agent reports $\alpha = \alpha_H$, the principal will deviate from the investment decisions under full information case by increasing the investment level. Such deviations result in the following consequences: the expected cost from breaches is reduced, and the agent's expected disutility from security breaches is reduced. Consequently, the principal does not need to compensate the agent for his disutility as much, the agent's salary in the α_H state is less than that under full information environment. On the contrary, the agent's salary in the α_L state is more than that under the full information environment, because the principal needs to provide the agent additional motivation to report the state truthfully.

As mentioned above, the principal believes that the agent is telling the truth when he reports $\alpha = \alpha_L$. One interesting question is that, would it be necessary for the principal to pre-commit to a security audit when the agent reports $\alpha = \alpha_L$? If it is not, with a costly security audit, the principal will always be better off by pre-committing to security audits only when the agent reports $\alpha = \alpha_H$. Under these circumstances, the principal would design the contracts in the following ways. She would minimize the same total cost as before, but subject to different constraints. Formally stated, the principal's problem, when $\eta = \alpha_H$, becomes

$$C_H = \min_{x_{HH}, S_{HH}, x_{HL}, S_{HL}} \left\{ \frac{\xi P_H}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_H, x_{HH}\right) L + x_{HH} + S_{HH} \right] \right.$$
$$\left. + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_L, x_{HL}\right) L + x_{HL} + S_{HL} \right] \right\}$$

subject to

$$\begin{aligned} S_{HH} - \beta P(\alpha_H, x_{HH}) L &\geq 0, && (2.17)\\ S_{HL} - \beta P(\alpha_L, x_{HL}) L &\geq 0, && (2.18)\\ S_{HH} - \beta P(\alpha_H, x_{HH}) L &\geq [S_{HL} - \beta P(\alpha_H, x_{HL}) L], && (2.19)\\ S_{HL} - \beta P(\alpha_L, x_{HL}) L &\geq (1-q)[S_{HH} - \beta P(\alpha_L, x_{HH}) L]. && (2.20) \end{aligned}$$

When $\eta = \alpha_L$,

$$C_L = \min_{x_{HH}, S_{HH}, x_{HL}, S_{HL}} \left\{ \frac{(1-\xi) P_H}{(1-\xi) P_H + \xi P_L} [P(\alpha_H, x_{LH}) L + x_{LH} + S_{LH}] + \frac{\xi P_L}{(1-\xi) P_H + \xi P_L} [P(\alpha_L, x_{LL}) L + x_{LL} + S_{LL}] \right\}$$

subject to

$$\begin{aligned} S_{LH} - \beta P(\alpha_H, x_{LH}) L &\geq 0, && (2.21)\\ S_{LL} - \beta P(\alpha_L, x_{LL}) L &\geq 0, && (2.22)\\ S_{LH} - \beta P(\alpha_H, x_{LH}) L &\geq [S_{LL} - \beta P(\alpha_H, x_{LL}) L], && (2.23)\\ S_{LL} - \beta P(\alpha_L, x_{LL}) L &\geq (1-q)[S_{LH} - \beta P(\alpha_L, x_{LH}) L]. && (2.24) \end{aligned}$$

Following the proof for the lemmas, one may find that the changed constraints are not binding, which means that the principal will offer the exact same contracts to the agent regardless of whether she would pre-commit to a security audit when the agent reports $\alpha = \alpha_L$. However, from the principal's point of view, not pre-committing is always more cost efficient than pre-committing to a security audit.

Proposition 2 *Given that a security audit is costly, it would be in the best interest of the principal to pre-commit to a security audit only when the agent reports that* $\alpha = \alpha_H$.

Another interesting result from proposition 1 is that the principal tends to overinvest in the high productivity case. This is not consistent with the conclusions from Harris and Raviv (1996). In their model, Harris and Raviv find that the principal tends to underinvest in high productivity project while overinvest in low productivity project. This is because that Harris and Raviv assume that the agent's salary is fixed regardless of the agent's message. By having a fixed salary, the principal can only affect the agent's payoffs by adjusting the investment level. In order to make sure the agent does not have the incentive to lie in his report, the principal would increase his payoff in low productivity case by overinvesting and decrease his payoff in high productivity case by underinvesting.

On the contrary, the current model assumes that the agent's salary is based on the report he submitted to the principal. In the high productivity case, the principal does not need to provide truth-telling motivation, hence the salary would be decreasing as the investment level increases. By overinvesting in high productivity case, the principal offers more investment but less salary to the agent. Thus, when the agent actually observes $\alpha = \alpha_L$ but reports $\alpha = \alpha_H$, he would benefit from receiving more investments but lose some of the salary. Since the salary is decreasing at the same rate as the investment would benefit the agent in the high productivity case, it is decreasing at a higher rate than the benefit in the low productivity case. Therefore, by overinvesting in the high productivity case, the principal actually reduces the payoff of the agent gets from lying when the true state is $\alpha = \alpha_L$.

Proposition 3 *If the difference in marginal cost savings of the investment between state α_H and α_L is a decreasing function of x, i.e., $P_x(\alpha_H, x) - P_x(\alpha_L, x)$ is an increasing function of x, then the principal will invest less in the high produc-*

tivity state when she observes $\eta = \alpha_H$ than she will when she observes $\eta = \alpha_L$; however, she will invest the same amount in low productivity state regardless the signal η she observes. The agent will receives more salary when the principal observes $\eta = \alpha_H$ and less salary when the principal observes $\eta = \alpha_L$, regardless of the true productivity state. i.e.,

$$\begin{aligned} \hat{x}_{HH} &\leq \hat{x}_{LH} \\ \hat{x}_{HL} &= \hat{x}_{LL} \\ \hat{S}_{HH} &\geq \hat{S}_{LH} \\ S_{HL} &\geq S_{LL}. \end{aligned}$$

Recall from proposition 1, only when $\alpha = \alpha_H$, the principal will deviate from the optimal investment decision rules by overinvesting in information security. As the principal's inferred probability of α_H being the true state increases, such deviation will become more costly. If the principal observes $\eta = \alpha_H$, she infers that it is more likely that α_H is the true state than she does under the case $\eta = \alpha_L$ is observed. Hence, the principal would overinvest to a lesser extent when she observes $\eta = \alpha_H$ than she would when she observes $\eta = \alpha_L$. As a result, she has to compensate the agent more for not investing as much when she observes $\eta = \alpha_H$.

Define information rent (IR) as the part of the agent's expected utility exceeding his reservation utility. Information rent measures how much the principal has to compensate the agent so that the agent will report truthfully. It can also be interpreted as the agent's payoff from possessing better information. Formally, when the true state is $\alpha = \alpha_H$, the expected information rent IR_H is

$$IR_H = \Pr(\eta = \alpha_H | \alpha = \alpha_H) \left[\hat{S}_{HH} - \beta P(\alpha_H, \hat{x}_{HH}) L\right]$$

$$+\Pr\left(\eta=\alpha_L|\alpha=\alpha_H\right)\left[\hat{S}_{LH}-\beta P\left(\alpha_H,\hat{x}_{LH}\right)L\right];$$

when the true state is $\alpha=\alpha_L$, the expected information rent IR_L is

$$\begin{aligned} IR_L &= \Pr\left(\eta=\alpha_H|\alpha=\alpha_L\right)\left[\hat{S}_{HL}-\beta P\left(\alpha_L,\hat{x}_{HL}\right)L\right] \\ &\quad +\Pr\left(\eta=\alpha_L|\alpha=\alpha_L\right)\left[\hat{S}_{LL}-\beta P\left(\alpha_L,\hat{x}_{LL}\right)L\right]. \end{aligned}$$

Proposition 4 *The agent receives no information rent when the true state is $\alpha=\alpha_H$, the agent receives positive information rent when the true state is $\alpha=\alpha_L$, i.e.,*

$$\begin{aligned} IR_H &= 0, \\ IR_H &> 0. \end{aligned}$$

The following propositions characterize the effects of information asymmetry and security audit intensity on principal's ex ante cost.

Proposition 5 *As information asymmetry decreases, principal's ex ante cost decreases, i.e.,*

$$\frac{\partial C}{\partial \xi}\leq 0.$$

As ξ increases, signal η provides more relevant information on α, and the information asymmetry between principal and agent decreases. The ex ante cost is decreasing in ξ, which means when the signal η becomes more precise, the principal expects to incur less total costs. Intuitively, the principal is more confident in her own signal, the burden of inducing the agent report truthfully is alleviated. Hence, the agency costs are reduced. The principal is in a better position when less information asymmetry exists.

Proposition 6 *As the intensity of a security audit increases, the principal's ex ante cost decreases, i.e.,*

$$\frac{\partial C}{\partial q} < 0.$$

This proposition suggests that there is a value to information security audits. Security audit provides the principal a certain chance to catch the agent lying. If the agent is found lying, he'll be removed and get zero utility. The agent's payoff from lying is thus reduced by security audits. This means if the principal commits to a certain security audit policy, the cost of motivating the agent to tell the truth will be reduced. As the security audit becomes more intensive, the chance of the principal catching the agent lying increases. As a result, the principal needs to pay less to motivate truthful reporting, and the investment decision rules are less distorted. The information security audits have value because they reduce the principal's ex ante costs. This does not imply that firms should always pursue the maximal security audit intensity. The above result has yet to consider the cost of security audits. As the audit intensity goes up, the cost of conducting security audits may also go up. It might even be prohibitively costly to conduct a security audit that provides the principal a hundred percent chance of catching the agent lying.

Proposition 7 *If in addition $P(\alpha, x)$ satisfies either*

$$P(\alpha, x) = P^{(1)}(\alpha) * P^{(2)}(x), \tag{2.25}$$

$$P^{(2)}_{xx}(x) \text{ is a monotonic function,}$$

or

$$\frac{P_x(\alpha_H, x) - P_x(\alpha_L, x)}{P_{xx}(\alpha_H, x)} \tag{2.26}$$

is a non-increasing function of x, then

$$\frac{\partial^2 C}{\partial q \partial \xi} \geq 0,$$

i.e., as information asymmetry decreases, the marginal benefit of security audit decreases.

Proposition 7 gives two sufficient conditions that the marginal benefit from security audit decreases as information asymmetry decreases. These conditions include wide classes of functions, such as exponential functions, log functions, inverse polynomial functions, etc. The conclusion is an interesting insight provided by the model. Although reducing information asymmetry and increasing security audit intensity both reduces the principal's costs, the marginal benefit of security audits decreases as the information asymmetry decreases.

2.5 Costs of Security Audits and Optimal Security Audit Intensity

The previous analyses show that security audits are beneficial to organizations in that they mitigate the negative impacts of information asymmetry between the principal and the agent. However, in order to determine the optimal level of a security audit, the model has yet to take the costs of security audits into considerations.

Naturally, when no security audit is conducted, i.e., the intensity of a security audit equals zero, the cost of security audits would be zero. As the security audit intensity is measured as the chance that the principal would catch the agent lying, one can imagine that the costs for security audits increase as such chance gets

greater. As the chance gets close to one, the costs of security audits may become prohibitive, as the audit may have to be able to eliminate most uncertainty the principal has about the system and the agent. In the extreme case, it may be even impossible to conduct a security audit that provides the principal a hundred percent chance to catch the agent lying. Therefore, the model assumes that the cost of security audits (K) is convex in security audit intensity. As the intensity of security audit approaches one, the cost of security audits approaches infinity. i.e.,

$$\begin{aligned} \frac{\partial K(q)}{\partial q} &> 0, \\ \frac{\partial^2 K(q)}{\partial q^2} &> 0, \\ K(0) &= 0, \\ \lim_{q \to 1} K(q) &\to \infty. \end{aligned}$$

As stated in proposition 7, the benefit of security audits also increases as the audit intensity increases. A close examination of the model reveals that the benefit is also convex in the audit intensity (detailed derivation can be found in the Appendix). As shown in the figures (2.3) and (2.4), there are two possible scenarios.

In Scenario 1, the cost of security audits is always greater than the benefits. As shown in the figure, the cost curve is always above the benefit curve and hence no security audit will happen. In Scenario 2, compared to the benefits, the cost of security audits increases slower at first, but faster as the audit intensity approaches to one. In some interval, the cost is less than the benefit, an optimal audit intensity which leads to maximum net benefits from security audits can be determined in this case. Given the popularity of security audits in practice, the

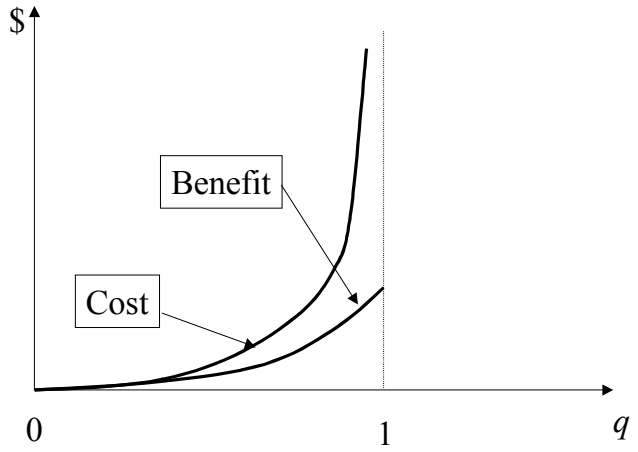


Figure 2.3: Scenario 1

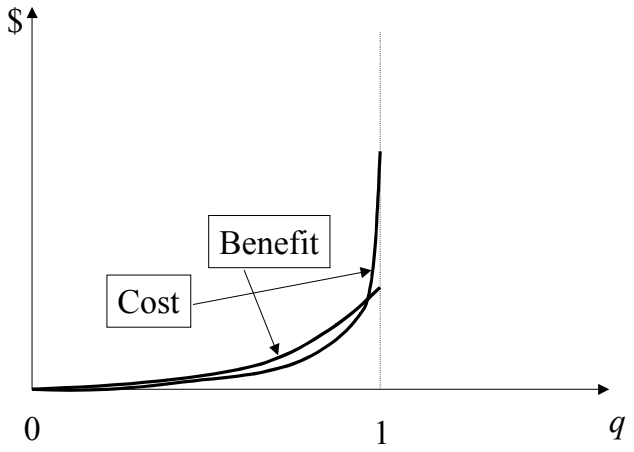


Figure 2.4: Scenario 2

model will further investigate the more interesting case, Scenario 2.

The discussion in last section assumes that the principal would pre-commit to a certain intensity of security audits. Since the principal observes a signal of the system's true state α before entering the contract, the principal can make the pre-commitment based on the signal observed. Assume the cost of security audits does not depend on the signal the principal observed. An interesting question to ask is when the principal will pre-commit to more security audits. Will the principal want to audit more when a bad signal, $\eta = \alpha_H$, is observed? Common sense may suggest that she will, since a bad signal means the principal has more to lose, and hence she may want to impose more control over the information system. However, the conventional wisdom is not supported by the following proposition.

Proposition 8 *The principal does not necessarily pre-commit to a more intensive security audit when she observes $\eta = \alpha_H$ than when she observes $\eta = \alpha_L$.*

2.6 A Special Case and Numerical Example

In order to provide closed-form solutions and more intuitive insights, this section gives a special case and numerical example of the model. Let

$$P(\alpha, x) = \frac{\alpha}{1+x}.$$

Figure 2.5 shows the graph of this probability function under different α. Figure 2.6 illustrates the marginal benefits $(-P_x(\alpha, x))$ of security investment under different α. As mentioned before, a greater α represents a worse-secured information system, but a more productive security investment.

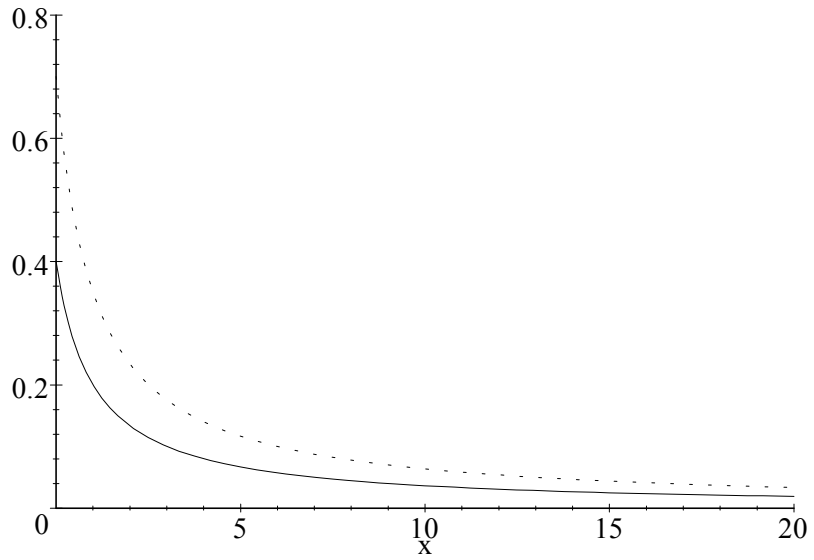


Figure 2.5: $P(\alpha, x)$ dots ($\alpha = 0.7$) and solid ($\alpha = 0.4$).

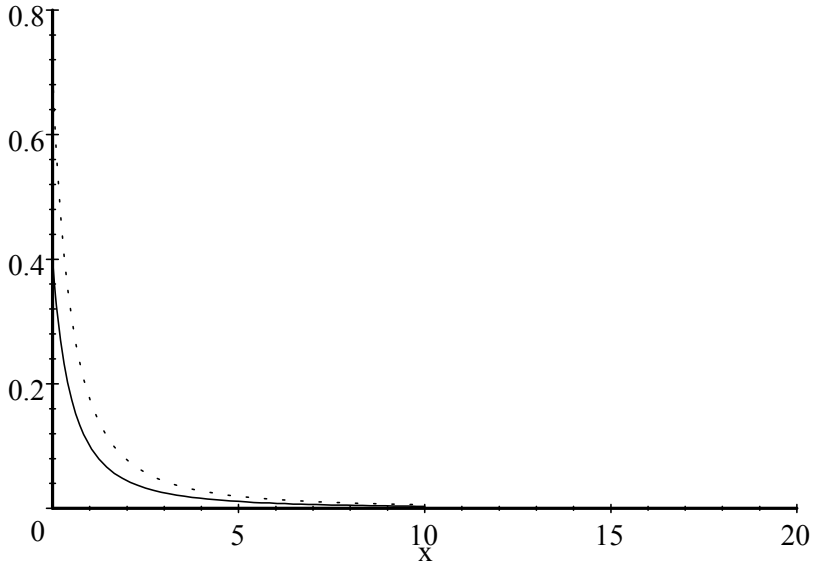


Figure 2.6: $-P_x(\alpha, x)$ dots ($\alpha = 0.7$) and solid ($\alpha = 0.4$)

As assumed by the model, information security investments reduce the probability of a security breach. Thus, for a given investment level, the system with a higher α always benefits more, but yields lower information security level. The closed-form solutions of this special case can be explicitly expressed as follows:

$$\begin{aligned}
\hat{x}_{HH} &= \sqrt{(1+\beta)\,\alpha_H L + \frac{(1-\xi)\,P_L}{\xi P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L} - 1,\\
\hat{x}_{HL} &= \sqrt{(1+\beta)\,\alpha_L L} - 1,\\
\hat{S}_{HH} &= \frac{\alpha_H \beta L}{\sqrt{(1+\beta)\,\alpha_H L + \frac{(1-\xi)P_L}{\xi P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L}},\\
\hat{S}_{HL} &= \frac{\alpha_L \beta L}{\sqrt{(1+\beta)\,\alpha_L L}} + \frac{(1-q)\,(\alpha_H-\alpha_L)\,\beta L}{\sqrt{(1+\beta)\,\alpha_H L + \frac{(1-\xi)P_L}{\xi P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L}},\\
\hat{x}_{LH} &= \sqrt{(1+\beta)\,\alpha_H L + \frac{\xi P_L}{(1-\xi)\,P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L} - 1,\\
\hat{x}_{LL} &= \sqrt{(1+\beta)\,\alpha_L L} - 1,\\
\hat{S}_{LH} &= \frac{\alpha_H \beta L}{\sqrt{(1+\beta)\,\alpha_H L + \frac{\xi P_L}{(1-\xi)P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L}},\\
\hat{S}_{LL} &= \frac{\alpha_L \beta L}{\sqrt{(1+\beta)\,\alpha_L L}} + \frac{(1-q)\,(\alpha_H-\alpha_L)\,\beta L}{\sqrt{(1+\beta)\,\alpha_H L + \frac{\xi P_L}{(1-\xi)P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L}}.
\end{aligned}$$

Hence the ex ante costs of the principal can be written as

$$\begin{aligned}
C &= \xi P_H\Big[\frac{(1+\beta)\,\alpha_H L}{\sqrt{(1+\beta)\,\alpha_H L + \frac{(1-\xi)P_L}{\xi P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L}}\\
&\quad + \sqrt{(1+\beta)\,\alpha_H L + \frac{(1-\xi)\,P_L}{\xi P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L} - 1\Big]\\
&\quad + (1-\xi)\,P_L\Big[2\sqrt{(1+\beta)\,\alpha_L L} - 1\\
&\quad + \frac{(1-q)\,(\alpha_H-\alpha_L)\,\beta L}{\sqrt{(1+\beta)\,\alpha_H L + \frac{(1-\xi)P_L}{\xi P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L}}\Big]\\
&\quad + (1-\xi)\,P_H\Big[\frac{(1+\beta)\,\alpha_H L}{\sqrt{(1+\beta)\,\alpha_H L + \frac{\xi P_L}{(1-\xi)P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L}}\\
&\quad + \sqrt{(1+\beta)\,\alpha_H L + \frac{\xi P_L}{(1-\xi)\,P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L} - 1\Big]
\end{aligned}$$

$$+\xi P_L[2\sqrt{(1+\beta)\,\alpha_L L}-1$$
$$+\frac{(1-q)\,(\alpha_H-\alpha_L)\,\beta L}{\sqrt{(1+\beta)\,\alpha_H L+\frac{\xi P_L}{(1-\xi)P_H}\,(1-q)\,(\alpha_H-\alpha_L)\,\beta L}}].$$

Some common parameters used in the following figures are presented below:

$$\begin{aligned}\alpha_H &= 0.7,\\ \alpha_L &= 0.4,\\ L &= 1000,\\ \beta &= 0.1.\end{aligned}$$

Figure 2.7 shows how the investment levels of $\hat{x}_{HH}$ and $\hat{x}_{LH}$ change as the information asymmetry measure ξ changes when the agent reports $\alpha = \alpha_H$. Recall that the principal overinvests when the agent reports $\alpha = \alpha_H$. If the principal observes $\eta = \alpha_H$, as ξ increases, the principal is more confident that α_H is the true state, overinvesting becomes more costly, hence, the principal will cut back the overinvestment. On the contrary, if the principal observes $\eta = \alpha_L$, as ξ increases, the principal believes that the chance of α_H being the true state is remote, overinvesting becomes less costly. Figure 2.8 shows how the investment levels of $\hat{x}_{HH}$ and $\hat{x}_{LH}$ change with the security audit intensity q when the agent reports $\alpha = \alpha_H$. Security audits provide the principal a chance to catch the agent lying, hence reduce the agent's incentive to report the false state. Thus the principal's investment decision rules become closer to those under full information case. The changes of investment levels of $\hat{x}_{HL}$ and $\hat{x}_{LL}$ when the true state is $\alpha = \alpha_L$ are not plotted because they are independent of ξ and q.

Figure 2.9 and 2.10 show how the agent's salary under various circumstances changes with the information asymmetry measure ξ changes. Since the agent always receives his reservation utility when $\alpha = \alpha_H$, overinvesting in information

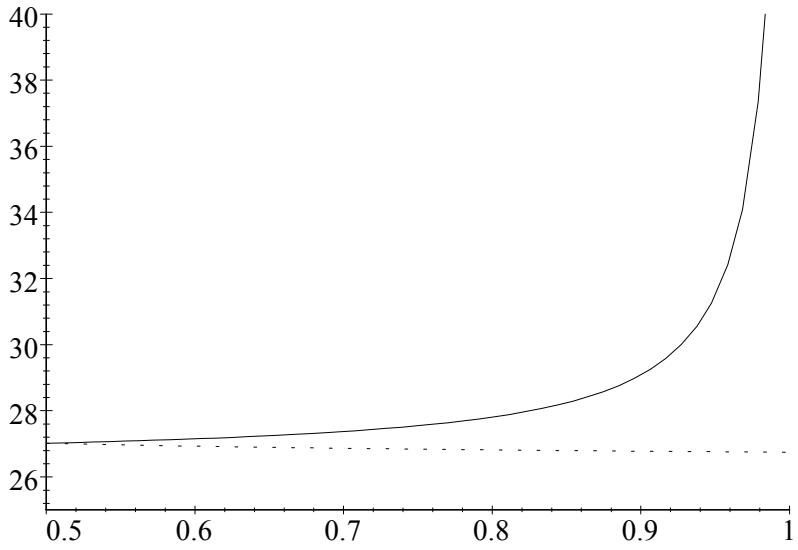


Figure 2.7: $\hat{x}_{HH}(\xi)$ (dots) and $\hat{x}_{LH}(\xi)$ (solid), where $q = \frac{1}{2}$, and $P_H = P_L = \frac{1}{2}$

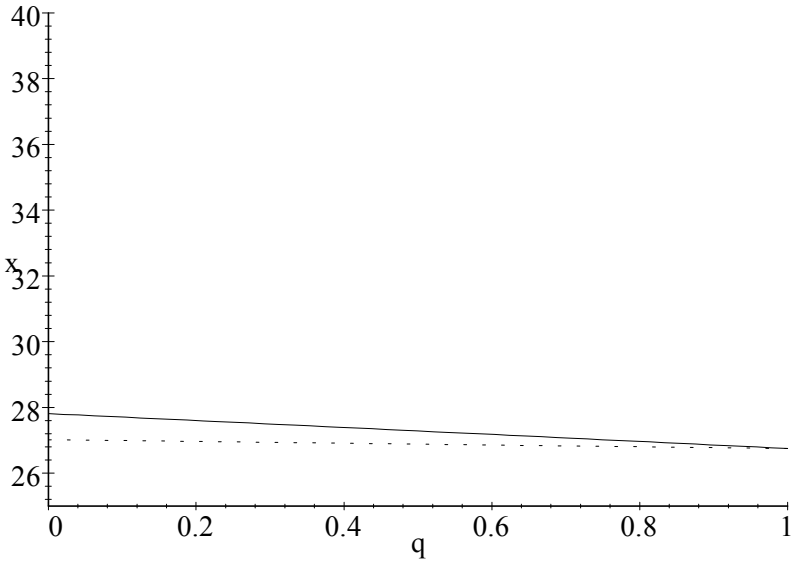


Figure 2.8: $\hat{x}_{HH}(q)$ (dots) and $\hat{x}_{LH}(q)$ (solid), where $\xi = \frac{2}{3}$ and $P_H = P_L = \frac{1}{2}$.

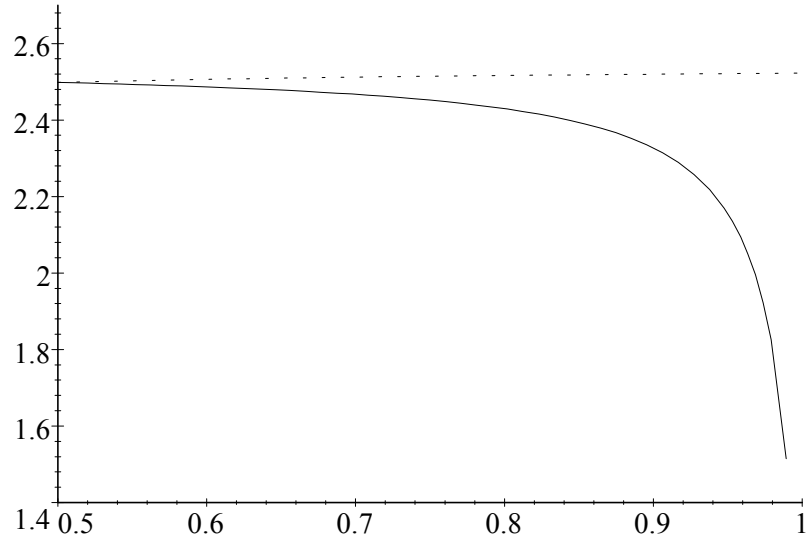


Figure 2.9: $\hat{S}_{HH}(\xi)$ (dots) and $\hat{S}_{LH}(\xi)$ (solid), $q = \frac{1}{2}$, $P_H = P_L = \frac{1}{2}$

security means the principal will pay less salary to the agent. Thus, $\hat{S}_{HH}$ and $\hat{S}_{LH}$ will always move in the opposite direction to $\hat{x}_{HH}$ and $\hat{x}_{LH}$.

Figure 2.11 and 2.12 plot how security audit intensity q affects the agent's salary. When q increases, the principal's investment decision rules deviate less from those in full information case. As a result, the agent's salaries also move to those under full information case.

Figure 2.13 plots the relation between information asymmetry ξ and the principal's ex ante costs and Figure 2.14 plots the relation between security audit intensity q and the principal's ex ante costs. Both figures confirm that the marginal benefit from security audits decreases as the information asymmetry decreases.

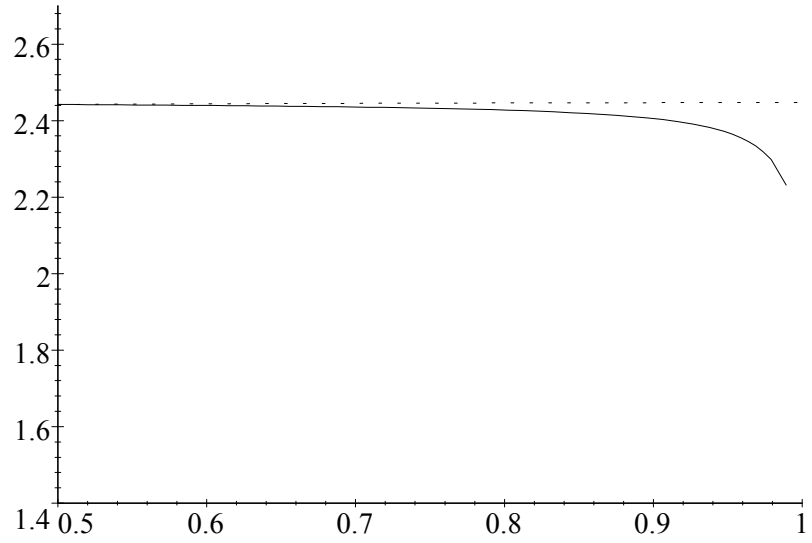


Figure 2.10: $\hat{S}_{HL}(\xi)$ (dots) and $\hat{S}_{LL}(\xi)$ (solid), $q = \frac{1}{2}$, $P_H = P_L = \frac{1}{2}$

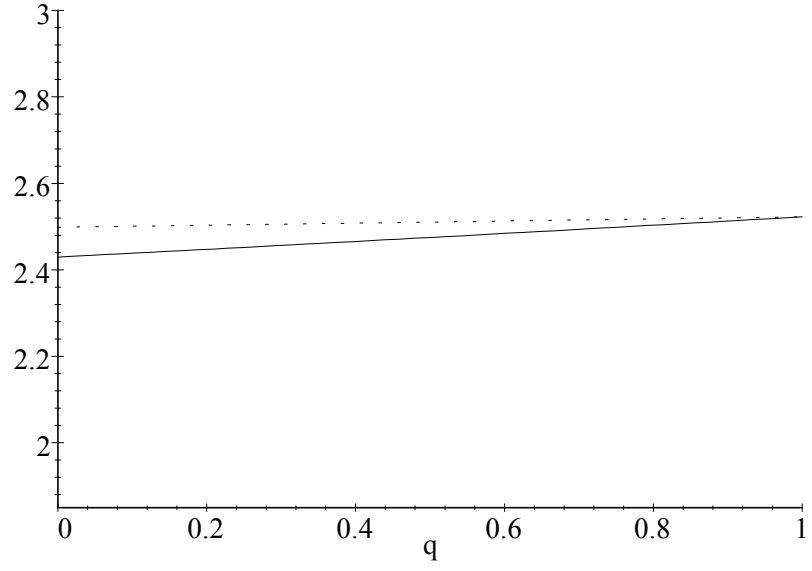


Figure 2.11: $\hat{S}_{HH}(q)$ (dots) and $\hat{S}_{LH}(q)$ (solid), $\xi = \frac{2}{3}$, $P_H = P_L = \frac{1}{2}$

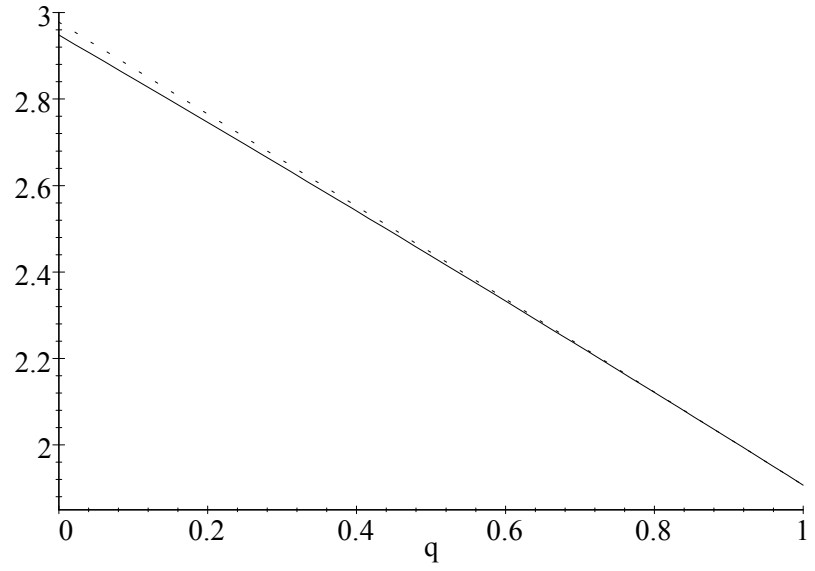


Figure 2.12: $\hat{S}_{HL}(q)$ (dots) and $\hat{S}_{LL}(q)$ (solid), $\xi = \frac{2}{3}$, $P_H = P_L = \frac{1}{2}$

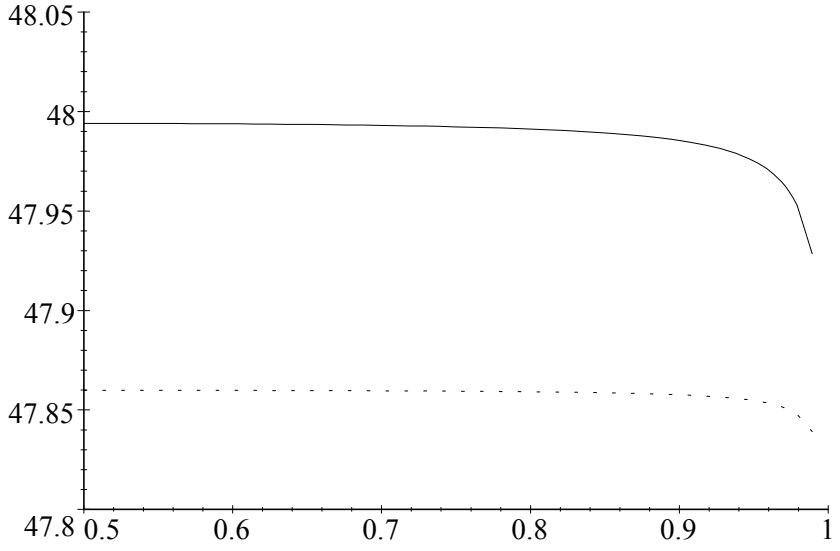


Figure 2.13: $C(\xi)$, solid ($q = \frac{1}{2}$) and dots ($q = \frac{3}{4}$), where $P_H = P_L = \frac{1}{2}$.

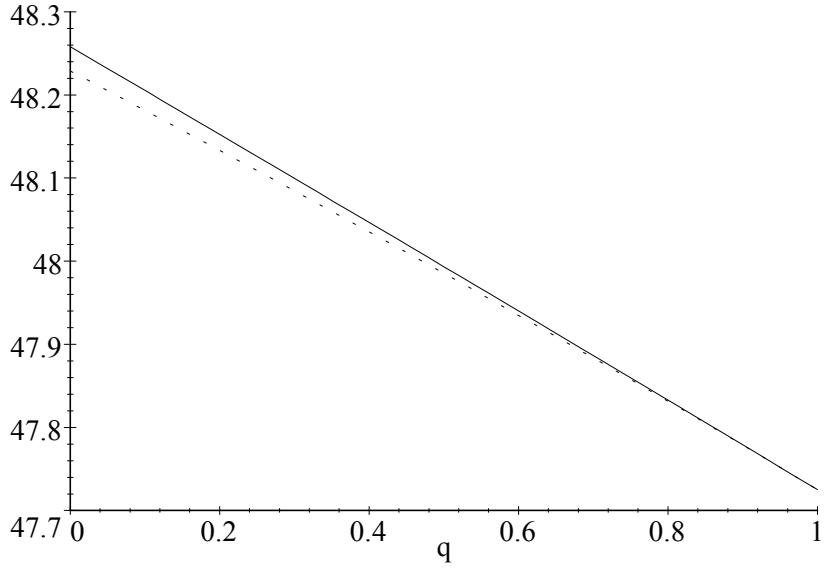


Figure 2.14: $C(q)$ solid ($\xi = \frac{2}{3}$) and dots ($\xi = \frac{9}{10}$), $P_H = P_L = 0.5$

Chapter 3

Market Impacts of Security Breaches

3.1 Methodology

3.1.1 Fama and French (1993) Three-Factor Model

The classical asset-pricing model suggests that a stock's return is a positive linear function of its market β (the slope in the regression of a stock's return on the market's return). By applying CAPM (Capital Asset Pricing Model, see Sharpe, 1964 and Lintner, 1965), researchers implicitly assume that β alone captures the systematic risk of stocks. However, empirical studies suggest that many other factors also have incremental explanatory power to market β for expected returns. These factors include size (Banz, 1981), financial leverage (Bhandari, 1988), book-to-market equity (Stattman, 1980, and Rosenberg, Reid and Lanstein, 1985) and earnings-price ratios (Basu, 1983 and Ball, 1978).

Fama and French (1992) cross-sectionally examine these factors. They find that while each of the factors alone does have explanatory power, two factors (size and book-to-market equity) combined seem to absorb the cross-sectional variation in average stock returns associated with all other factors. Fama and

French (1993) conduct time-series tests and identify three common risk factors in the returns on stocks. These three risk factors are excess market returns, size and book-to-market equity. Fama and French argue that the risks of stocks are multidimensional, a one-factor model like CAPM can capture only one dimension of the risks. Although the underlying risks associated with size and book-to-equity have yet to be identified, combining these two factors into return regressions seems to help incorporating other dimensions of the risks and yields better results. Formally stated, Fama and French propose the following three-factor regression model to explain securities' returns:

$$R(t) - RF(t) = a + b[RM(t) - RF(t)] + sSMB(t) + hHML(t) + e(t)$$

where

$R(t)$ = the return to be explained over time period t;

$RF(t)$ = the risk-free rate over time period t;

$RM(t)$ = value-weighted return on market portfolio over time period t;

$SMB(t)$ = (small minus big) the difference between the return on a portfolio of small stocks and the return on a portfolio of large stocks over time peirod t;

$HML(t)$ = (high minus low) the differenct btween the return on a portfolio of high-book-to-market stocks and the return on a portfolio of low-book-to-market stocks over time period t.

Fama and French (1996) continue the line of this research by showing that most asset pricing anomalies can be explained by the three-factor model proposed in Fama and French (1993).

In the following part of this study, the three-factor regression model of Fama and French (1993) will be used to capture the market's expectation of stocks' returns, as it can more precisely reflect the multidimensional risks and provide more rigorous conclusions.

3.1.2 Hypothesis Development

This study first examines the overall economic effects of publicly announced security breach events. Campbell et al. (2003) state that there is no significant market reaction to public reports of information security breaches. The following null hypothesis $\mathbf{H1_0}$ tests if such conclusion applies to the extended sample.

$H1_0$: There is no stock market reaction to public reports of corporate information security breaches.

Campbell et al. (2003) show that security incidents involving breaches of confidential information on average have significant negative market reactions, while non-confidential security incidents do not have significant market reactions. With a bigger sample and a more sophisticated model, these statements can be examined with more confidence. The full sample is divided into two sub-samples: i.e., information security breach events involving breaches of confidential information and those not involving breaches of confidential events. Hypotheses $\mathbf{H2_A}$ and $\mathbf{H2_B}$ examine the market reactions of each sub-sample respectively.

$H2_A$: There is no stock market reaction to public reports of corporate information security breaches involving unauthorized access to confidential information.

$H2_B$: There is no stock market reaction to public reports of corporate information security breaches that do not involve unauthorized

access to confidential information.

Some researchers (Garg et al., 2003) suggest that computer virus incidents should be excluded from the event study sample because computer viruses are general in nature and it is hard to specify which firms were infected and the exact date of the outbreaks. During the event search of this study, 32 information security breach incidents were identified as being associated with computer viruses. Each event is announced with clear specifications of firms affected and date of virus infections. Thus the non-confidential event sub-sample is further partitioned into two categories: computer virus related events and non-computer virus related events. Hypotheses $\mathbf{H3_A}$ and $\mathbf{H3_B}$ address the market reactions to each group of events.

$\mathbf{H3_A}$: There is no stock market reaction to public reports of non-confidential corporate information security breaches involving computer viruses.

$\mathbf{H3_B}$: There is no stock market reaction to public reports of non-confidential corporate information security breaches that do not involve computer viruses.

3.1.3 Sample Selection

The publicly announced information security breach events were identified by electronically searching the full text of ten major newspapers over the time period from January 1, 1995 to December 31, 2002. Besides the five news paper included in Campbell et al. (2003) (*Wall Street Journal*, *New York Times*, *Washington Post*, *Financial Times* and *USA Today*), additional five newspapers (*Boston Globe*, *Chicago Sun-Times*, *Houston Chronicle*, *Los Angeles Times* and

San Francisco Chronicle) were added in the extended search. All the newspapers are among the top 20 largest circulations, the newly added five newspapers also present a regional distribution across the United States. The keywords in the search include: "information security breach", "computer system security", "hacker", "cyber attack", "computer attack", "computer break-in" and "computer virus".

The search returned 159 information security breach events associated with US corporations. In order to study the stock price reactions to these events, the following criteria are imposed. To be included in the final sample, each affected firm must have a sufficiently long history of return data available on the Center of Research in Security Prices (CRSP) database, and the events must be announced within a month after the breaches actually happened. Additionally, there should be no mergers or acquisitions occurring during either the estimation periods or test windows. For firms with multiple breach events, only those events for which the estimation periods do not overlap previous breaches are included. For information breaches that happened after September 11, 2001, the estimation periods must not overlap with the 9/11 attack. Only 71 events qualify all the sample selection criteria. Table 1 provides the impacts of each criterion on our sample size.

Table1 SampleSelectionCriteria

Criteria	Impact	Remaining
Initial number of security breaches	159	159
CRSP data availability	(51)	108
Events occurred within a month of announcement	(6)	102
Estimation period covers 9/11	(9)	93
Overlapping multiple security breaches	(14)	79
Short history or mergers	(8)	71

Table 2 lists all the events in the final sample. Based on the nature of the breached information, each event in the final sample is identified as "Confidential" breach or "Non-confidential" breach. The 9 "Confidential" events involve unauthorized access to confidential information, e.g. unauthorized access to credit card data, unauthorized access to customer's personal data, etc. The remaining 62 events do not involve unauthorized access to confidential information. Among the 62 non-confidential events, over half (32) events are security breaches involving computer viruses and the rest (30) are information security incidents that did not involve computer viruses.

Table 3 presents the industry distribution of the firms. Several firms had multiple security breaches, therefore, though there are 71 information security breach events, there are only 62 firms in the sample. The 62 firms come from 15 different industries, including both high-tech industries and traditional manufacturing or service industries. Industrial clustering poses a potential issue in the sample since there are 20 firms from the business service industry.

All the return data are collected from the CRSP/Compustat Merged Database.

Following from Fama and French (1993,1996), the explanatory returns R_M, SMB, and HML are formed as follows. At the end of each year (1994-2001), NYSE, AMEX and Nasdaq stocks are all divided into two groups (small or big, S or B) based on whether their year-end market equity (ME, stock price times shares outstanding) is below or above the median ME for NYSE stocks. NYSE, AMEX and Nasdaq stocks are allocated into three book-to-market equity (BE/ME) groups (low, medium, or high; L, M, or H) based on the breakpoints for the bottom 30 percent, middle 40 percent and top 30 percent of the values of BE/ME for NYSE stocks. Six size-BE/ME portfolios (S/L, S/M, S/H, B/L, B/M and B/H) are defined as the intersections of the two ME and the three BE/ME groups. Value-weighted daily returns on each portfolio are calculated for the following year. SMB is the difference between the average of the returns on the three small-stock portfolios (S/L, S/M and S/H) and the average of the return on the three big-stock portfolios (B/L, B/M and B/H). HML is the difference between the average of the returns on the two high-BE/ME portfolios (S/H and B/H) and the average of the returns on the two low-BE/ME portfolios (S/L and B/L). R_M is the value-weighted return on NYSE/AMEX/Nasdaq stocks[1].

[1]BE is the book value of stockholder's equity, plus balance sheet deferred taxes and investment tax credit, minus the book value of preferred stock. Firms with negative BEs were excluded when the size-BE/ME portfolios were formed.

Table 2 Sample information security breach events

Company name	Source	Date	Confidentiality	Event description
Ford Motor Credit Company	New York Times	05/17/02	Confidential	Unauthorized use of authorization code
Vivendi Universal	Financial Times	04/27/02	Non-confidential	Unauthorized access to electronic voting system
Interland Inc	Washington Post	03/21/02	Non-confidential	Unauthorized website entry & alteration
Verisign Inc	Washington Post	03/21/02	Non-confidential	Unauthorized website entry & alteration
Citigroup	Financial Times	09/06/01	Non-confidential	Unauthorized service interruption
Qwest Communications	USA Today	08/20/01	Non-confidential	"Code Red" worm
AT & T Corp.	USA Today	08/20/01	Non-confidential	"Code Red" worm
FedEx Corp	Wall Street Journal	08/09/01	Non-confidential	"Code Red" worm
Ask Jeeves Inc. (Excite.com)	USA Today	08/09/01	Non-confidential	"Code Red" worm
Cox Communications	USA Today	08/09/01	Non-confidential	"Code Red" worm
A O L Time Warner Inc	USA Today	08/09/01	Non-confidential	"Code Red" worm
Dow Jones & Co.	Wall Street Journal	07/20/01	Non-confidential	"Code Red" worm
DoubleClick Inc.	Wall Street Journal	03/30/01	Non-confidential	Unauthorized website entry
Egghead.com Inc	Washington Post	12/23/00	Confidential	Unauthorized access to credit card data
Disney	USA Today	09/27/00	Confidential	Unauthorized access to Disney World guest data
First Data Corp. (Western Union)	Wall Street Journal	09/11/00	Confidential	Unauthorized acess to credit & debit card data
Nike Inc	Wall Street Journal	06/22/00	Non-confidential	Unauthorized traffic re-direction
TicketMaster Online Citysearch	USA Today	05/05/00	Non-confidential	love bug
Cognos Inc	USA Today	05/05/00	Non-confidential	love bug
Bear Stearns Cos	USA Today	05/05/00	Non-confidential	love bug
Trans World Airlines Inc.	USA Today	05/05/00	Non-confidential	love bug
Estee Lauder Cos	Wall Street Journal	05/05/00	Non-confidential	love bug
Ford Motor Corp	Wall Street Journal	05/05/00	Non-confidential	love bug
Barnes & Noble	Wall Street Journal	05/05/00	Non-confidential	love bug
Vodafone Group PLC (Vodafone AirTouch)	Financial Times	05/05/00	Non-confidential	love bug
AT & T Corp.	Chicago Sun-Times	05/05/00	Non-confidential	love bug
National Discount Brokers	Wall Street Journal	02/25/00	Non-confidential	Unauthorized service interruption
McGraw-Hill Cos	Wall Street Journal	02/22/00	Confidential	Unauthorized access to confidential info by employee
Aastrom Biosciences Inc.	Wall Street Journal	02/18/00	Non-confidential	Unauthorized website entry & alteration
PairGain Technologies Inc.	Wall Street Journal	02/18/00	Non-confidential	Unauthorized website entry & alteration
MCI WorldCom Inc	Wall Street Journal	02/10/00	Non-confidential	Denial of service
CNET Networks Inc (ZDNet)	Wall Street Journal	02/10/00	Non-confidential	Denial of service
About.com	Wall Street Journal	02/10/00	Non-confidential	Denial of service
Time warner Inc (CNN)	Washington Post	02/09/00	Non-confidential	Denial of service
Amazon.com Inc.	Wall Street Journal	02/09/00	Non-confidential	Denial of service

Company name	Source	Date	Confidentiality	Event description
Charles Schwab Corp	Wall Street Journal	02/08/00	Non-confidential	Denial of service
Yahoo!	Wall Street Journal	02/08/00	Non-confidential	Denial of service
Lycos	Financial Times	02/08/00	Non-confidential	Denial of service
E-Trade Group	USA Today	02/08/00	Non-confidential	Denial of service
eBay Inc.	USA Today	02/08/00	Non-confidential	Denial of service
Drug Emporium Inc.	Wall Street Journal	01/31/00	Confidential	Unauthorized access to credit card data
America Online	Wall Street Journal	01/27/00	Non-confidential	Flaw in email system
Northwest Airlines Corp	Wall Street Journal	01/10/00	Confidential	Unauthorized access to credit card data
Banc of America	San Francisco Chronicle	12/02/99	Non-confidential	Minizip virus
Dell Computer Corp	Financial Times	11/19/99	Non-confidential	Production interruption by virus
Critical Path Inc.	Wall Street Journal	09/22/99	Non-confidential	Flaw in email system
Symantec Corp	Houston Chronicle	08/06/99	Non-confidential	Unauthorized website entry & alteration
Network Solutions Inc	Washington Post	07/03/99	Non-confidential	Unauthorized webstie entry & traffic redirection
Electronic Arts Inc. (Maxis Studios)	Wall Street Journal	06/14/99	Non-confidential	Worm.Explore.Zip virus
Motorola	Chicago Sun-Times	06/13/99	Non-confidential	Worm.Explore.Zip virus
AT& T Corp.	Financial Times	06/12/99	Non-confidential	Worm.Explore.Zip virus
Lehman Brothers Holdings Inc.	Financial Times	06/12/99	Non-confidential	Worm.Explore.Zip virus
Boeing co.	Financial Times	06/12/99	Non-confidential	Worm.Explore.Zip virus
General Electric	Boston Globe	06/11/99	Non-confidential	Worm.Explore.Zip virus
Playboy Enterprises International	Chicago Sun-Times	03/30/99	Non-confidential	Melissa Virus
Chevron Corp	San Francisco Chronicle	03/30/99	Non-confidential	Melissa Virus
Northrop Grumman Corp.	Wall Street Journal	03/30/99	Non-confidential	Melissa Virus
Merrill Lynch & Co. Inc	USA Today	03/30/99	Non-confidential	Melissa Virus
Compaq Computer Corp	USA Today	03/30/99	Non-confidential	Melissa Virus
Lockheed Martin Corp	USA Today	03/30/99	Non-confidential	Melissa Virus
Intel Corp.	New York Times	03/29/99	Non-confidential	Melissa Virus
Charles Schweb & Company	New York Times	03/29/99	Non-confidential	Melissa Virus
Lucent Technologies	New York Times	03/29/99	Non-confidential	Melissa Virus
Microsoft Corp.	Wall Street Journal	10/27/98	Confidential	Unauthorized access to subscriber data
America Online	Wall Street Journal	10/19/98	Non-confidential	Unauthorized alteration of services address
New York Times Co.	Wall Street Journal	09/14/98	Non-confidential	Unauthorized webstie entry & alteration
America Online	Wall Street Journal	01/05/98	Confidential	Unauthorized access to passwords/credit card data
Yahoo!	Chicago Sun-Times	12/10/97	Non-confidential	Unauthorized website entry & alteration
Microsoft Corp.	Wall Street Journal	06/23/97	Non-confidential	Unauthorized service intterruption
America Online	San Francisco Chronicle	02/07/97	Non-confidential	Unauthorized service interruption
New York Times	Boston Globe	08/04/95	Non-confidential	Unauthorized service interruption

Table 3 Sample industry distribution

SIC	Industry description	No. of firms
1700	Construction special trade contractors	1
2700	Printing, publising & allied industries	4
2800	Chemicals & allied products	2
2900	Petroleum refining & related industries	1
3000	Rubber & miscellaneous plastics products	1
3500	Industrial & commercial machinery & computer equipment	2
3600	Electronic & other electrical equipment & components, except computer equipment	4
3700	Transportation equipment	5
4500	Transportation by air	3
4800	Communications	6
5900	Miscellaneous retail	2
6000	Depository institutions	1
6100	Non-depository credit institutions	1
6200	Security & commodity brokers, dealers, exchanges & services	6
7300	Business Service	20
7800	Motion pictures	3
	Total	62

3.1.4 Research Design

Like Campbell et al. (2003), this study uses both the ordinary least square (OLS) regression and seemingly unrelated regression (SUR) to estimate the parameters. Standard event study approaches mainly use OLS methodology. OLS requires the error terms from regressions are independently identically distributed. However, there are some industry clustering as well as some event clustering (e.g., the denial-of-service attack events in February 2000 and some computer virus events) in the sample. To address the possible heteroskedasticity and intercorrelated error term issues in the sample, this study also adopts SUR method in regressions.

OLS Methodology

Following directly from Fama and French (1993), the expected return of each individual firm is fitted by

$$R_{it} = a_i + b_i R_{Mt} + s_i SMB_t + h_i HML_t + \varepsilon_{it},$$

where:

R_{it} = return for firm i's stock on day t, net of the risk-free rate;

R_{mt} = return for the market on day t, net of the risk-free rate;

SMB_t = the difference between the return on a portfolio of small stocks and the return of on a portfolio of large stocks on day t;

HML_t = the differenct btween the return on a portfolio of high-book-to-market stocks and the return on a portfolio of low-book-to-market stocks on day t;

a_i, b_i, s_i, h_i = intercept and slope parameters for firm i;

ε_{it} = disturbance term.

The parameters $\hat{a}_i, \hat{b}_i, \hat{s}_i, \hat{h}_i$ are estimated using an estimation period of 120 days. For each security breach incident, the estimation period starts 121 trading days before the event announcement and ends 2 trading days before the announcement. The abnormal returns for each event day are then computed as follows:

$$AR_{it} = R_{it} - \left(\hat{a}_i + \hat{b}_i R_{Mt} + \hat{s}_i SMB_t + \hat{h}_i HML_t\right).$$

The abnormal returns (AR) reflects differences between the realized returns on event days and the market expected returns for each individual firm, thus can be thought as a measurement of impact of security breaches on the market. A three-day event window, which includes the announcement day, previous trading day and subsequent trading day, is used to capture the whole impact of an information security breach. The cumulated abnormal return for firm i (CAR_i) over the event windows is then computed as follows:

$$CAR_i = \sum_{t=t_1}^{t_2} AR_{it},$$

where

$$[t_1, t_2] = \text{the event interval.}$$

The average announcement effect across events can be measured by

$$\overline{CAR} = \frac{1}{N} \sum_{i=1}^{N} CAR_i.$$

where N = the number of events.

SUR Methodology

The SUR method is one type of Generalized Least Squares (GLS) models and as mentioned above, is used in this study to address the heteroskedasticity and clustering issues in the sample. To be more specific, for the 71 events in the sample, the SUR model goes as follows:

$$\begin{aligned} R_{1t} &= a_1 + b_1 R_{Mt} + s_1 SMB_t + h_1 HML_t + \gamma_1 D + \varepsilon_{1t}, \\ R_{2t} &= a_2 + b_2 R_{Mt} + s_2 SMB_t + h_2 HML_t + \gamma_2 D + \varepsilon_{2t}, \\ &\vdots \\ R_{Nt} &= a_N + b_N R_{Mt} + s_N SMB_t + h_N HML_t + \gamma_N D + \varepsilon_{Nt}, \end{aligned}$$

where $D = 1$ if within the 3 day event period $[-1, +1]$, and 0 otherwise.

The coefficient γ_i is used to capture the abnormal returns on the event days and follow the example of OLS method, the average effects of the events can then be computed as:

$$\overline{\gamma} = \frac{1}{N} \sum_{i=1}^{N} \gamma_i,$$

if there is no significant market reaction to the information security breach events, it is expected that $\overline{\gamma} = 0$.

3.2 Results

Table 4 shows the results from OLS method. Although in all cases mean CARs have negative sign, for the full sample, the null hypothesis that there were no market reactions to the reports of security breaches cannot be rejected. The Z-statistic is only marginally significant in this case. When the full sample is split into two categories, confidential events and non-confidential events, the

results show that for confidential event sub-sample the market has a significant reaction (mean $CAR = -0.0502$) to the reports of information security breaches, while for the non-confidential events, the market has no significant reaction to the reports of security breaches. These results verify those of Campbell et al. (2003).

In order to exclude the possibility that the insignificance of non-confidential events is caused by inclusions of computer virus related events in the sample, the non-confidential events are further partitioned into two groups, virus related and non-virus related information security incidents. The tests show no significant market reactions for either group. Thus one can conclude that the insignificance of non-confidential events is not driven by the inclusion of computer virus related events. Further dividing the non-confidential events based on whether they were computer virus related does not seem to provide additional insights on the economic impacts of information security breaches.

Table 4: Results from OLS method

	N	Mean CAR	Z-stat	% negative CARs
Panel A (*full sample*)				
Full sample	71	−0.0140	−1.5443	60.56
Panel B (*sample partitions based on confidentiality*)				
Confidential events	9	−0.0502	−2.3009	66.67
Non-confidential events	62	−0.0088	−0.8867	54.84
Panel C (*sample partitions based on virus*)				
Virus events	32	−0.0056	−0.5397	59.38
Non-virus events	30	−0.0122	−0.7070	50.00

The results from SUR method (as shown in table 5) further confirm the findings from OLS regressions. After controlling the possible heteroskedasticity and intercorrelation problems, SUR derives similar results to those of OLS. The F-value (2.30) for the whole sample is still not significant ($\Pr > F = 0.1292$), thus one cannot reject the hypothesis that there is no market reaction to the reported security breaches. For the confidential events, however, the F-value (5.17) is significant ($\Pr > F = 0.0230$) to reject the hypothesis that there is no market reaction to the reports of security breaches. In contrast, for non-confidential events, the F-value is again insignificant ($\Pr > F = 0.3755$). Further partitioning the sample into virus-related events and non virus-related events shows that neither group caused significant market reactions.

Table 5: Results from SUR method

	Avg. Hypothesis (avg. coeff=0)
Panel A (*full sample*)	
F-value	2.30
Pr $> F$	0.1292
D.F.	1
	8378
Panel B (*confidential event sub-sample*)	
F-Value	5.17
Pr $> F$	0.0230
D.F.	1
	8378
Panel C (*non-confidentail event sub-sample*)	
F-Value	0.79
Pr $> F$	0.3755
D.F.	1
	8378

Table 5 Results from SUR method (cont'd)

	Avg. Hypothesis (avg. coeff=0)
Panel D (*virus related non-confidential event sub-sample*)	
F-value	0.41
Pr $> F$	0.5236
D.F.	1
	8378
Panel E (*other non-confidential event sub-sample*)	
F-value	0.44
Pr $> F$	0.5091
D.F.	1
	8378

Chapter 4

Conclusion

4.1 Information Security Audits and Asymmetric Information

Using a principal-agent model, the first part of this dissertation examines the interactions between information asymmetry and security audits during the security investment process. Although the model is developed for a security investment environment, the setup and conclusions can be easily applied to other scenarios of capital investments and audits (i.e., information security audits can be thought of as sub-class of various types of audits).

Consistent with a common practice of security audits, the model suggests that a security audit does have value to a firm due to information asymmetry between different levels of management. Under asymmetric information, the principal (e.g., firm's CEO principal) will deviate from the optimal investment rules in order to motivate truthful reports from the agent (e.g., the CISO). More specifically, the principal tends to over-invest, when compared with the symmetric information case, in security projects with high productivity, but

sticks to the optimal investment rules when the productivity is low. The CISO (i.e., the agent), who possesses more precise information than the CEO (i.e., the principal) and always prefers more investments than the CEO, has an incentive to lie in his report when the productivity is low. As a result, the agent will receive information rent when the true productivity is low as a reward for reporting the truth. Information security audits act to both mitigate such deviations and reduce the CISO's payoff from false reports.

There are limitations of the model presented in this dissertation, which represent directions for future research. The most obvious of these limitations are the need to model the costs of information security audits and the agent's effort level. These limitations notwithstanding, the current model provides useful insights into the relations among information security auditing, information asymmetry and firm value.

4.2 Impacts of Information Security Breaches

The second part of this dissertation extends the earlier work of Campbell et al. (2003) by examining the market reactions to publicly announced information security breaches from 1995 to 2002. A more sophisticated model is used to capture the market's expectation of stock returns. Our results are consistent with those of Campbell et al. (2003). Overall, the market only has marginal negative reaction to reports of information security breach events. Partitioning the events based on the confidentiality of the information breached revealed a clearer picture. For those reports of events involving unauthorized access to confidential information, the market shows a statistically significant negative

price reaction. On the contrary, no significant market reaction was induced by reports of non-confidential information security incidents. In summary, there are three major contributions of this extension study:

First, a more rigorous approach is used to estimate the abnormal returns of the events. Unlike the single factor model used in Campbell et al. (2003), a three-factor model (Fama and French, 2003) is used to capture the behavior of stock returns. It gives a more precise estimate of the abnormal return, which is the key statistic used in this research. The results from this approach confirmed the conclusions of Campbell et al. (2003).

Second, to investigate if the insignificance of non-confidential events is the result of inclusion of computer virus-related events in the sample, this study further examines the market reactions to non-virus non-confidential events and virus-related non-confidential events. The tests show that the market has no significant price reactions to the announcements of either type of events. This finding proves that the market reaction to non-confidential security breaches is not likely to be affected by whether the security breaches are caused by computer viruses.

Finally, this study extends the sample of Campbell et al. (2003). Five more major newspaper and additional two years (2001-2002) were included in the search process. The results suggest the conclusions of Campbell et al. (2003) apply to a larger sample and do not seem to change over the last several years.

Chapter 5

Table of Notations

- α : the state of information system, may take two values, α_H or α_L.
- P_H : the chance that α equals α_H.
- P_L : the chance that α equals α_L.
- $\hat{\alpha}$: the agent's report on α.
- η : the principal's signal on α.
- ξ : the chance that η equals α.
- x : the level of information security investments. x_H^* is the optimal level of security investments when $\alpha = \alpha_H$ and there's no information asymmetry; x_L^* is the optimal level of security investments when $\alpha = \alpha_L$ and there's no information asymmetry. When there does exist information asymmetry, $\hat{x}_{HH}$ is the optimal level of security investments when the principal observes $\eta = \alpha_H$ and the agent reports $\hat{\alpha} = \alpha_H$; $\hat{x}_{HL}$ is the optimal level of security investments when $\eta = \alpha_H$ and $\hat{\alpha} = \alpha_L$; $\hat{x}_{LH}$ is the optimal level of security

investments when $\eta = \alpha_L$ and $\hat{\alpha} = \alpha_H$; and $\hat{x}_{LL}$ is the optimal level of security investments when $\eta = \alpha_L$ and $\hat{\alpha} = \alpha_L$.

- $P(\alpha, x)$: the probability of an information security breach.
- L : the principal's loss from a realized information security breach.
- β : the extent to which the agent suffers from a security breach, βL represents the agent's disutility from a security breach.
- S : the agent's salary. $\hat{S}_{HH}$ is the optimal salary (from the principal's point of view) when the principal observes $\eta = \alpha_H$ and the agent reports $\hat{\alpha} = \alpha_H$; $\hat{S}_{HL}$ is the optimal salary when $\eta = \alpha_H$ and $\hat{\alpha} = \alpha_L$; $\hat{S}_{LH}$ is the optimal salary when $\eta = \alpha_L$ and $\hat{\alpha} = \alpha_H$; and $\hat{S}_{LL}$ is the optimal salary when $\eta = \alpha_L$ and $\hat{\alpha} = \alpha_L$.
- q : the intensity of a security audit.
- IR : information rent. IR_H is the expected information rent when the true state is $\alpha = \alpha_H$, and IR_L is the expected information rent when the true state is $\alpha = \alpha_L$.
- $K(q)$: the cost of an information security audit with audit intensity q.

Chapter 6

Appendix

6.1 Proof of Lemma 1

First consider the case when the principal observes $\eta = \alpha_H$.

From constraint (2.5)

$$S_{HH} - \beta P(\alpha_H, x_{HH}) L \geq 0.$$

Since $\alpha_H > \alpha_L$, it follows that

$$P(\alpha_H, x_{HH}) > P(\alpha_L, x_{HH}) > 0$$

and

$$S_{HH} - \beta P(\alpha_L, x_{HH}) L > S_{HH} - \beta P(\alpha_H, x_{HH}) L,$$

hence

$$S_{HH} - \beta P(\alpha_L, x_{HH}) L > 0,$$

which means

$$S_{HL} - \beta P(\alpha_L, x_{HL}) L \geq (1-q)[S_{HH} - \beta P(\alpha_L, x_{HH}) L] > 0.$$

Therefore, constraint (2.6) is redundant and constraint (2.8) binds.

Similarly, one can show that constraint (2.10) is redundant and constraint (2.12) binds.

6.2 Proof of Lemma 2

Again, first consider the case when the principal observes $\eta = \alpha_H$.

Remember $\alpha_H > \alpha_L$, it also follows that

$$P(\alpha_H, x_{HL}) > P(\alpha_L, x_{HL}) > 0,$$

and

$$S_{HL} - \beta P(\alpha_L, x_{HL}) L > S_{HL} - \beta P(\alpha_H, x_{HL}) L.$$

If constraint (2.5) binds, it implies

$$S_{HL} - \beta P(\alpha_L, x_{HL}) L = 0,$$

but

$$S_{HL} - \beta P(\alpha_L, x_{HL}) L > S_{HL} - \beta P(\alpha_H, x_{HL}) L.$$

Thus constraint (2.7) becomes redundant. Therefore, only one of constraints (2.5) and (2.7) binds. The following proof will show that the minimized objective function based on constraint (2.5) is always less than the minimized objective function based on constraint (2.7), therefore constraint (2.7) is redundant.

Notice that if constraint (2.5) binds,

$$S_{HL} - \beta P(\alpha_H, x_{HL}) L \leq 0;$$

if constraint (2.7) binds,

$$S_{HL} - \beta P(\alpha_H, x_{HL}) L > 0.$$

From constraint (2.5), one can see

$$S_{HH} \geq \beta P\left(\alpha_H, x_{HH}\right) L.$$

Assume constraint (2.7) binds, it implies

$$S_{HL} \geq \beta P\left(\alpha_H, x_{HL}\right) L.$$

Hence, the objective function

$$\begin{aligned}
& \frac{\xi P_H}{\xi P_H + (1-\xi) P_L}\left[P\left(\alpha_H, x_{HH}\right) L + x_{HH} + S_{HH}\right] \\
& + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}\left[P\left(\alpha_L, x_{HL}\right) L + x_{HL} + S_{HL}\right] \\
\geq\ & \frac{\xi P_H}{\xi P_H + (1-\xi) P_L}\left[P\left(\alpha_H, x_{HH}\right) L + x_{HH} + \beta P\left(\alpha_H, x_{HH}\right) L\right] \\
& + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}\left[P\left(\alpha_L, x_{HL}\right) L + x_{HL} + \beta P\left(\alpha_H, x_{HL}\right) L\right].
\end{aligned}$$

Let

$$\begin{aligned}
g \ =\ & \frac{\xi P_H}{\xi P_H + (1-\xi) P_L}\left[P\left(\alpha_H, x_{HH}\right) L + x_{HH} + \beta P\left(\alpha_H, x_{HH}\right) L\right] \\
& + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}\left[P\left(\alpha_L, x_{HL}\right) L + x_{HL} + \beta P\left(\alpha_H, x_{HL}\right) L\right].
\end{aligned}$$

One can always find $\tilde{x}_{HH}$ and $\tilde{x}_{HL}$ that minimize g. $\tilde{x}_{HH}$ and $\tilde{x}_{HL}$ must satisfy the following first order conditions:

$$\begin{aligned}
(1+\beta) P_x\left(\alpha_H, x_{HH}\right) L + 1 &= 0, \\
P_x\left(\alpha_L, x_{HL}\right) L + \beta P_x\left(\alpha_H, x_{HL}\right) L + 1 &= 0.
\end{aligned}$$

Given

$$P_x\left(\alpha_L, \tilde{x}_{HL}\right) > P_x\left(\alpha_H, \tilde{x}_{HL}\right),$$

it follows directly that

$$\begin{aligned}
(1+\beta) P_x\left(\alpha_H, \tilde{x}_{HH}\right) &= P_x\left(\alpha_L, \tilde{x}_{HL}\right) + \beta P_x\left(\alpha_H, \tilde{x}_{HL}\right) \\
&> (1+\beta) P_x\left(\alpha_H, \tilde{x}_{HL}\right). \qquad (6.1)
\end{aligned}$$

Combined with

$$P_{xx}(\alpha, x) > 0,$$

inequality (6.1) implies that

$$\tilde{x}_{HH} > \tilde{x}_{HL}.$$

Now assume constraint (2.5) binds, it follows

$$S_{HH} = \beta P(\alpha_H, x_{HH}) L,$$

and from constraint (2.8),

$$S_{HL} = \beta P(\alpha_L, x_{HL}) L + (1-q)[S_{HH} - \beta P(\alpha_H, x_{HH}) L].$$

The objective function can be written as

$$\begin{aligned}
& \frac{\xi P_H}{\xi P_H + (1-\xi) P_L}[P(\alpha_H, x_{HH}) L + x_{HH} + S_{HH}] \\
& + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}[P(\alpha_L, x_{HL}) L + x_{HL} + S_{HL}] \\
= & \frac{\xi P_H}{\xi P_H + (1-\xi) P_L}[P(\alpha_H, x_{HH}) L + x_{HH} + \beta P(\alpha_H, x_{HH}) L] \\
& + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}\{P(\alpha_L, x_{HL}) L + x_{HL} + \beta P(\alpha_L, x_{HL}) L \\
& + (1-q)[S_{HH} - \beta P(\alpha_H, x_{HH}) L]\},
\end{aligned}$$

which is always equal to or less than

$$\begin{aligned}
f = & \frac{\xi P_H}{\xi P_H + (1-\xi) P_L}[P(\alpha_H, x_{HH}) L + x_{HH} + \beta P(\alpha_H, x_{HH}) L] \\
& + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}[P(\alpha_L, x_{HL}) L + x_{HL} + \beta P(\alpha_L, x_{HL}) L \\
& + S_{HH} - \beta P(\alpha_H, x_{HH}) L].
\end{aligned}$$

Now compare g and f valued at $\tilde{x}_{HH}$ and $\tilde{x}_{HL}$:

$$(g-f)|_{\tilde{x}_{HH}, \tilde{x}_{HL}}$$

$$
\begin{aligned}
= & \frac{\xi P_H}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_H, \tilde{x}_{HH}\right) L + \tilde{x}_{HH} + \beta P\left(\alpha_H, \tilde{x}_{HH}\right) L \right] \\
& + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_L, \tilde{x}_{HL}\right) L + \tilde{x}_{HL} + \beta P\left(\alpha_H, \tilde{x}_{HL}\right) L \right] \\
& - \frac{\xi P_H}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_H, \tilde{x}_{HH}\right) L + \tilde{x}_{HH} + \beta P\left(\alpha_H, \tilde{x}_{HH}\right) L \right] \\
& - \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} [P\left(\alpha_L, \tilde{x}_{HL}\right) L + \tilde{x}_{HL} + \beta P\left(\alpha_L, \tilde{x}_{HL}\right) L \\
& + \beta P\left(\alpha_H, \tilde{x}_{HH}\right) L - \beta P\left(\alpha_L, \tilde{x}_{HH}\right) L] \\
= & \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} [\beta P\left(\alpha_H, \tilde{x}_{HL}\right) L - \beta P\left(\alpha_L, \tilde{x}_{HL}\right) L \\
& - \beta P\left(\alpha_H, \tilde{x}_{HH}\right) L + \beta P\left(\alpha_L, \tilde{x}_{HH}\right) L].
\end{aligned}
$$

Since

$$
\begin{aligned}
\tilde{x}_{HH} &> \tilde{x}_{HL}, \\
P\left(\alpha_H, \hat{x}_{HH}\right) - P\left(\alpha_H, \tilde{x}_{HL}\right) &= \int_{\tilde{x}_{HL}}^{\hat{x}_{HH}} P_x(\alpha_H, x) dx, \\
P\left(\alpha_L, \tilde{x}_{HH}\right) - P\left(\alpha_L, \tilde{x}_{HL}\right) &= \int_{\tilde{x}_{HL}}^{\hat{x}_{HH}} P_x(\alpha_L, x) dx,
\end{aligned}
$$

recall that

$$
P_x\left(\alpha_H, x\right) < P_x\left(\alpha_L, x\right),
$$

it follows that

$$
P\left(\alpha_H, \hat{x}_{HH}\right) - P\left(\alpha_H, \tilde{x}_{HL}\right) < P\left(\alpha_L, \tilde{x}_{HH}\right) - P\left(\alpha_L, \tilde{x}_{HL}\right),
$$

i.e.,

$$
P\left(\alpha_H, \tilde{x}_{HL}\right) - P\left(\alpha_L, \tilde{x}_{HL}\right) > P\left(\alpha_H, \tilde{x}_{HH}\right) - P\left(\alpha_L, \tilde{x}_{HH}\right),
$$

hence

$$
\begin{aligned}
& (g-f)\left|_{\tilde{x}_{HH}, \tilde{x}_{HL}}\right. \\
> & \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} [\beta P\left(\alpha_H, \tilde{x}_{HH}\right) L - \beta P\left(\alpha_L, \tilde{x}_{HH}\right) L
\end{aligned}
$$

$$
\begin{aligned}
& -\beta P\left(\alpha_H, \tilde{x}_{HH}\right) L + \beta P\left(\alpha_L, \tilde{x}_{HH}\right) L] \\
= \; & 0.
\end{aligned}
$$

Note that the minimized objective function using constraints (2.7) and (2.8) is always greater than or equal to g valued at $(\tilde{x}_{HH}, \tilde{x}_{HL})$, and the minimized objective function using constraints (2.5) and (2.8) is always less than or equal to f valued at $(\tilde{x}_{HH}, \tilde{x}_{HL})$. Therefore, the minimized objective function based on constraints (2.7) and (2.8) is greater than the minimized objective function based on constraints (2.5) and (2.8). Hence, constraint (2.7) is redundant and constraint (2.5) binds.

Similar proofs can be applied when the principal observes $\eta = \alpha_L$, and conclude that constraint (2.9) is redundant and constraint (2.9) binds.

6.3 Proofs of Propositions

Eliminating the redundant constraints, the principal needs to solve the following problem when $\eta = \alpha_H$ is observed

$$
\begin{aligned}
C_H = & \min_{x_{HH}, S_{HH}, x_{HL}, S_{HL}} \{ \frac{\xi P_H}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_H, x_{HH}\right) L + x_{HH} + S_{HH} \right] \\
& + \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_L, x_{HL}\right) L + x_{HL} + S_{HL} \right] \}
\end{aligned}
$$

subject to

$$
\begin{aligned}
S_{HH} - \beta P\left(\alpha_H, x_{HH}\right) L & \geq 0. \\
S_{HL} - \beta P\left(\alpha_L, x_{HL}\right) L & \geq (1-q) \left[S_{HH} - \beta P\left(\alpha_L, x_{HH}\right) L \right].
\end{aligned}
$$

The following procedures use Lagrangian method. The Lagrangian function $\pounds$ can be written as

$$\begin{aligned}
\pounds &= -\frac{\xi P_H}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_H, x_{HH}\right) L + x_{HH} + S_{HH} \right] \\
&\quad -\frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} \left[P\left(\alpha_L, x_{HL}\right) L + x_{HL} + S_{HL} \right] \\
&\quad +\lambda_{H1} \left[S_{HH} - \beta P\left(\alpha_H, x_{HH}\right) L \right] + \lambda_{H2} \{ S_{HL} \\
&\quad -\beta P\left(\alpha_L, x_{HL}\right) L - (1-q) \left[S_{HH} - \beta P\left(\alpha_L, x_{HH}\right) L \right] \}. \qquad (6.2)
\end{aligned}$$

The first order conditions maximizing Lagrangian function (6.2) are:

$$\begin{aligned}
\frac{\partial \pounds}{\partial x_{HH}} &= -\frac{\xi P_H}{\xi P_H + (1-\xi) P_L} \left[P_x\left(\alpha_H, x_{HH}\right) L + 1 \right] \\
&\quad +\lambda_{H1} \left[-\beta P_x\left(\alpha_H, x_{HH}\right) L \right] + \lambda_{H2} (1-q) \beta P_x\left(\alpha_L, x_{HH}\right) L \\
&= 0, \\
\frac{\partial \pounds}{\partial x_{HL}} &= -\frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} \left[P_x\left(\alpha_L, x_{HL}\right) L + 1 \right] \\
&\quad +\lambda_{H2} \left[-\beta P_x\left(\alpha_L, x_{HL}\right) L \right] \\
&= 0, \\
\frac{\partial \pounds}{\partial S_{HH}} &= -\frac{\xi P_H}{\xi P_H + (1-\xi) P_L} + \lambda_{H1} - \lambda_{H2} (1-q) = 0, \\
\frac{\partial \pounds}{\partial S_{HL}} &= -\frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} + \lambda_{H2} = 0, \\
\frac{\partial \pounds}{\partial \lambda_{H1}} &= S_{HH} - \beta P\left(\alpha_H, x_{HH}\right) L = 0, \\
\frac{\partial \pounds}{\partial \lambda_{H2}} &= S_{HL} - \beta P\left(\alpha_L, x_{HL}\right) L - (1-q) \left[S_{HH} - \beta P\left(\alpha_L, x_{HH}\right) L \right] = 0.
\end{aligned}$$

The solutions to the above equations are:

$$\begin{aligned}
\hat{\lambda}_{H1} &= \frac{\xi P_H}{\xi P_H + (1-\xi) P_L} + (1-q) \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} > 0, \\
\hat{\lambda}_{H2} &= \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} > 0;
\end{aligned}$$

for $\hat{x}_{HH}$:

$$
\begin{aligned}
&-\frac{\xi P_H}{\xi P_H + (1-\xi) P_L} \left[P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1\right] \\
&+\left[\frac{\xi P_H}{\xi P_H + (1-\xi) P_L} + (1-q) \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}\right] \left[-\beta P_x\left(\alpha_H, \hat{x}_{HH}\right) L\right] \\
&+\frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} (1-q) \beta P_x\left(\alpha_L, \hat{x}_{HH}\right) L = 0, \\
&\left[P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1\right] + \left[1 + (1-q) \frac{(1-\xi) P_L}{\xi P_H}\right] \beta P_x\left(\alpha_H, \hat{x}_{HH}\right) L \\
&-(1-q) \frac{(1-\xi) P_L}{\xi P_H} \beta P_x\left(\alpha_L, \hat{x}_{HH}\right) L = 0, \\
&(1+\beta) P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1 \\
&+(1-q) \frac{(1-\xi) P_L}{\xi P_H} \beta L \left[P_x\left(\alpha_H, \hat{x}_{HH}\right) - P_x\left(\alpha_L, \hat{x}_{HH}\right)\right] = 0;
\end{aligned} \tag{6.3}
$$

for $\hat{x}_{HL}$:

$$
\begin{aligned}
-\frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} &\left[P_x(\alpha_L, \hat{x}_{HL}) L + 1\right] \\
+\frac{-(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} &\beta P_x\left(\alpha_L, \hat{x}_{HL}\right) L = 0,
\end{aligned}
$$

$$
\begin{aligned}
P_x\left(\alpha_L, x_{HL}\right) L + 1 + \beta P_x\left(\alpha_L, \hat{x}_{HL}\right) L &= 0, \\
(1+\beta) P_x\left(\alpha_L, x_{HL}\right) L + 1 &= 0;
\end{aligned} \tag{6.4}
$$

for $\hat{S}_{HH}$ and $\hat{S}_{HL}$:

$$
\hat{S}_{HH} = \beta P\left(\alpha_H, \hat{x}_{HH}\right) L, \tag{6.5}
$$

$$
\hat{S}_{HL} = \beta P\left(\alpha_L, \hat{x}_{HL}\right) L + (1-q)\left[\hat{S}_{HH} - \beta P\left(\alpha_L, \hat{x}_{HH}\right) L\right]. \tag{6.6}
$$

Similarly, when the principal observes $\eta = \alpha_L$, the solutions satisfy the following conditions:

for $\hat{x}_{LH}$:

$$
\begin{aligned}
&(1+\beta) P_x\left(\alpha_H, \hat{x}_{LH}\right) L + 1 \\
&+(1-q) \frac{\xi P_L}{(1-\xi) P_H} \beta L \left[P_x\left(\alpha_H, \hat{x}_{LH}\right) - P_x\left(\alpha_L, \hat{x}_{LH}\right)\right] = 0;
\end{aligned} \tag{6.7}
$$

for $\hat{x}_{LL}$:

$$(1+\beta)\, P_x\left(\alpha_L, \hat{x}_{LL}\right) L + 1 = 0; \tag{6.8}$$

for $\hat{S}_{LH}$ and $\hat{S}_{LL}$:

$$\begin{aligned} \hat{S}_{LH} &= \beta P\left(\alpha_H, \hat{x}_{LH}\right) L, & (6.9)\\ \hat{S}_{LL} &= \beta P\left(\alpha_L, \hat{x}_{LL}\right) L + (1-q)\left[S_{LH} - \beta P\left(\alpha_L, \hat{x}_{LH}\right) L\right]. & (6.10) \end{aligned}$$

6.3.1 Proof of Proposition 1

From equation (6.3) and equation (2.1) and the fact that

$$P_x\left(\alpha_H, \hat{x}_{HH}\right) < P_x\left(\alpha_L, \hat{x}_{HH}\right),$$

then

$$\begin{aligned} & (1+\beta)\, P_x\left(\alpha_H, x_H^*\right) L + 1 \\ = \; & (1+\beta)\, P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1 \\ & + (1-q)\, \frac{(1-\xi)\, P_L}{\xi P_H} \beta L \left[P_x\left(\alpha_H, \hat{x}_{HH}\right) - P_x\left(\alpha_L, \hat{x}_{HH}\right)\right] \\ < \; & (1+\beta)\, P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1. \end{aligned}$$

Combined with

$$P_{xx}\left(\alpha, x\right) > 0,$$

it follows that

$$\hat{x}_{HH} > x_H^*.$$

From equation (2.3) and equation (6.4)

$$(1+\beta)\, P_x\left(\alpha_H, x_L^*\right) L + 1 = (1+\beta)\, P_x\left(\alpha_H, \hat{x}_{HL}\right) L + 1,$$

which implies

$$\hat{x}_{HL} = x_L^*.$$

Given

$$\begin{aligned} \hat{x}_{HH} &> x_H^*, \\ \hat{x}_{HL} &= x_L^*, \end{aligned}$$

from equation (2.2) and equation (6.5), one can conclude that

$$\hat{S}_{HH} < S_H^*,$$

from equation (2.4) and equation (6.6), one can conclude that

$$\hat{S}_{HL} > S_L^*.$$

The proofs of $\hat{x}_{LH} > x_H^*$, $\hat{x}_{LL} = x_L^*$, $\hat{S}_{LH} < S_H^*$, $\hat{S}_{LL} > S_L^*$ follows the similar arguments without any difficulty.

6.3.2 Proof of Proposition 3

Recall $\xi \geq \frac{1}{2}$, which implies

$$\frac{\xi P_L}{(1-\xi) P_H} \leq \frac{(1-\xi) P_L}{\xi P_H}.$$

From equations (6.3) and (6.7),

$$\begin{aligned} & (1+\beta) P_x(\alpha_H, \hat{x}_{HH}) L + 1 \\ & + (1-q) \frac{(1-\xi) P_L}{\xi P_H} \beta L \left[P_x(\alpha_H, \hat{x}_{HH}) - P_x(\alpha_L, \hat{x}_{HH}) \right] \\ = \; & (1+\beta) P_x(\alpha_H, \hat{x}_{LH}) L + 1 \\ & + (1-q) \frac{\xi P_L}{(1-\xi) P_H} \beta L \left[P_x(\alpha_H, \hat{x}_{LH}) - P_x(\alpha_L, \hat{x}_{LH}) \right]. \end{aligned} \tag{6.11}$$

Assume

$$\hat{x}_{HH} > \hat{x}_{LH},$$

then

$$P_x\left(\alpha_H, \hat{x}_{HH}\right) - P_x\left(\alpha_L, \hat{x}_{HH}\right) \geq P_x\left(\alpha_H, \hat{x}_{LH}\right) - P_x\left(\alpha_L, \hat{x}_{LH}\right),$$

this leads to

$$\begin{aligned}
& (1+\beta) P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1 \\
& + (1-q) \frac{(1-\xi) P_L}{\xi P_H} \beta L \left[P_x\left(\alpha_H, \hat{x}_{HH}\right) - P_x\left(\alpha_L, \hat{x}_{HH}\right)\right] \\
\geq\ & (1+\beta) P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1 \\
& + (1-q) \frac{(1-\xi) P_L}{\xi P_H} \beta L \left[P_x\left(\alpha_H, \hat{x}_{LH}\right) - P_x\left(\alpha_L, \hat{x}_{LH}\right)\right]. \qquad (6.12)
\end{aligned}$$

Since

$$P_x\left(\alpha_H, x\right) - P_x\left(\alpha_L, x\right) < 0,$$

it follows that

$$\begin{aligned}
& (1+\beta) P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1 \\
& + (1-q) \frac{(1-\xi) P_L}{\xi P_H} \beta L \left[P_x\left(\alpha_H, \hat{x}_{LH}\right) - P_x\left(\alpha_L, \hat{x}_{LH}\right)\right] \\
\geq\ & (1+\beta) P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1 \\
& + (1-q) \frac{\xi P_L}{(1-\xi) P_H} \beta L \left[P_x\left(\alpha_H, \hat{x}_{LH}\right) - P_x\left(\alpha_L, \hat{x}_{LH}\right)\right], \qquad (6.13)
\end{aligned}$$

recall

$$P_{xx}\left(\alpha, x\right) > 0,$$

thus

$$\begin{aligned}
& (1+\beta) P_x\left(\alpha_H, \hat{x}_{HH}\right) L + 1 \\
& + (1-q) \frac{\xi P_L}{(1-\xi) P_H} \beta L \left[P_x\left(\alpha_H, \hat{x}_{LH}\right) - P_x\left(\alpha_L, \hat{x}_{LH}\right)\right]
\end{aligned}$$

$$
\begin{aligned}
> \quad & (1+\beta) P_x(\alpha_H, \hat{x}_{LH}) L + 1 \\
& + (1-q) \frac{\xi P_L}{(1-\xi) P_H} \beta L \left[P_x(\alpha_H, \hat{x}_{LH}) - P_x(\alpha_L, \hat{x}_{LH}) \right]. \qquad (6.14)
\end{aligned}
$$

Combine inequalities (6.12), (6.13) and (6.14), it follows that

$$
\begin{aligned}
& (1+\beta) P_x(\alpha_H, \hat{x}_{HH}) L + 1 \\
& + (1-q) \frac{(1-\xi) P_L}{\xi P_H} \beta L \left[P_x(\alpha_H, \hat{x}_{HH}) - P_x(\alpha_L, \hat{x}_{HH}) \right] \\
> \quad & (1+\beta) P_x(\alpha_H, \hat{x}_{LH}) L + 1 \\
& + (1-q) \frac{\xi P_L}{(1-\xi) P_H} \beta L \left[P_x(\alpha_H, \hat{x}_{LH}) - P_x(\alpha_L, \hat{x}_{LH}) \right].
\end{aligned}
$$

This contradicts equation (6.11), therefore, the assumption

$$\hat{x}_{HH} > \hat{x}_{LH}$$

is invalid. One can conclude that

$$\hat{x}_{HH} \leq \hat{x}_{LH}.$$

From equations (6.5), (6.6), (6.9), (6.10), and

$$P_x(\alpha, x) < 0,$$

it can be easily shown that

$$
\begin{aligned}
\hat{S}_{HH} &\geq \hat{S}_{LH}, \\
\hat{S}_{HL} &\geq \hat{S}_{LL}.
\end{aligned}
$$

The result of $\hat{x}_{HL} = \hat{x}_{LL}$ follows directly from proposition 1.

6.3.3 Proof of Proposition 4

From first order conditions (6.5) and (6.9),

$$IR_H = \Pr(\eta = \alpha_H | \alpha = \alpha_H) \left[\hat{S}_{HH} - \beta P(\alpha_H, \hat{x}_{HH}) L \right]$$

$$
\begin{aligned}
&+\Pr\left(\eta=\alpha_L|\alpha=\alpha_H\right)\left[\hat{S}_{LH}-\beta P\left(\alpha_H,\hat{x}_{LH}\right)L\right]\\
=\;& 0.
\end{aligned}
$$

From first order conditions (6.6) and (6.10),

$$
\begin{aligned}
IR_L =\;& \Pr\left(\eta=\alpha_H|\alpha=\alpha_L\right)\left[\hat{S}_{HL}-\beta P\left(\alpha_L,\hat{x}_{HL}\right)L\right]\\
&+\Pr\left(\eta=\alpha_L|\alpha=\alpha_L\right)\left[\hat{S}_{LL}-\beta P\left(\alpha_L,\hat{x}_{LL}\right)L\right]\\
=\;& (1-\xi)(1-q)\left[\hat{S}_{HH}-\beta P\left(\alpha_L,\hat{x}_{HH}\right)L\right]\\
&+\xi(1-q)\left[S_{LH}-\beta P\left(\alpha_L,\hat{x}_{LH}\right)L\right]\\
=\;& (1-q)(1-\xi)\beta L\left[P\left(\alpha_H,\hat{x}_{HH}\right)-P\left(\alpha_L,\hat{x}_{HH}\right)\right]\\
&+(1-q)\xi\beta L\left[P\left(\alpha_H,\hat{x}_{LH}\right)-P\left(\alpha_L,\hat{x}_{LH}\right)\right]\\
>\;& 0.
\end{aligned}
$$

6.3.4 Proof of Proposition 5

Principal's ex ante cost

$$
C=\left[\xi P_H+(1-\xi)P_L\right]C_H+\left[(1-\xi)P_H+\xi P_L\right]C_L. \tag{6.15}
$$

By Envelope theorem

$$
\begin{aligned}
\frac{\partial C}{\partial \xi} =\;& P_H\left[P\left(\alpha_H,\hat{x}_{HH}\right)L+\hat{x}_{HH}+\hat{S}_{HH}\right]-P_L\left[P\left(\alpha_L,\hat{x}_{HL}\right)L+\hat{x}_{HL}+\hat{S}_{HL}\right]\\
&-P_H\left[P\left(\alpha_H,\hat{x}_{LH}\right)L+\hat{x}_{LH}+\hat{S}_{LH}\right]+P_L\left[P\left(\alpha_L,\hat{x}_{LL}\right)L+\hat{x}_{LL}+\hat{S}_{LL}\right]\\
=\;& P_H\left[P\left(\alpha_H,\hat{x}_{HH}\right)L+\hat{x}_{HH}+\hat{S}_{HH}-P\left(\alpha_H,\hat{x}_{LH}\right)L-\hat{x}_{LH}-\hat{S}_{LH}\right]\\
&+P_L\left(\hat{S}_{LL}-\hat{S}_{HL}\right)\\
=\;& P_H\left[(1+\beta)P\left(\alpha_H,\hat{x}_{HH}\right)L+\hat{x}_{HH}-(1+\beta)P\left(\alpha_H,\hat{x}_{LH}\right)L-\hat{x}_{LH}\right]\\
&+P_L\left(\hat{S}_{LL}-\hat{S}_{HL}\right).
\end{aligned} \tag{6.16}
$$

Recall

$$\hat{x}_{HH} > x_H^*,$$

$$\hat{x}_{LH} > x_H^*,$$

Notice that when

$$x \geq x_H^*,$$

function

$$(1+\beta) P(\alpha, x) L + x$$

is increasing in x. Since

$$\hat{x}_{HH} \leq \hat{x}_{LH},$$

it follows that

$$(1+\beta) P(\alpha_H, \hat{x}_{HH}) L + \hat{x}_{HH} \leq (1+\beta) P(\alpha_H, \hat{x}_{LH}) L + \hat{x}_{LH}.$$

Combined with

$$\hat{S}_{HL} \geq \hat{S}_{LL},$$

these lead to

$$\frac{\partial C}{\partial \xi} \leq 0.$$

6.3.5 Proof of Proposition 6

From (6.15),

$$\frac{\partial C}{\partial q} = [\xi P_H + (1-\xi) P_L] \frac{\partial C_H}{\partial q} + [(1-\xi) P_H + \xi P_L] \frac{\partial C_L}{\partial q}.$$

By envelope theorem:

$$\frac{\partial C_H}{\partial q} = -\frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} \left(\hat{S}_{HH} - \beta P(\alpha_L, \hat{x}_{HH}) L \right).$$

Recall

$$\left(\hat{S}_{HH} - \beta P\left(\alpha_L, \hat{x}_{HH}\right) L\right) > \left(\hat{S}_{HH} - \beta P\left(\alpha_H, \hat{x}_{HH}\right) L\right) = 0,$$

thus,

$$\frac{\partial C_H}{\partial q} < 0.$$

Similarly,

$$\frac{\partial C_L}{\partial q} < 0.$$

It follows that

$$\frac{\partial C}{\partial q} < 0.$$

6.3.6 Proof of Proposition 7

Note

$$\frac{\partial^2 C}{\partial q \partial \xi} = \frac{\partial^2 C}{\partial \xi \partial q}.$$

From equation (6.16), it follows

$$\begin{aligned}
&\frac{\partial C}{\partial \xi} \\
= \;& P_H\left[(1+\beta) P\left(\alpha_H, \hat{x}_{HH}\right) L + \hat{x}_{HH} - (1+\beta) P\left(\alpha_H, \hat{x}_{LH}\right) L - \hat{x}_{LH}\right] \\
& + P_L\{\beta P\left(\alpha_L, \hat{x}_{LL}\right) L + (1-q)\left[S_{LH} - \beta P\left(\alpha_L, \hat{x}_{LH}\right) L\right] \\
& - \beta P\left(\alpha_L, \hat{x}_{HL}\right) L - (1-q)\left[S_{HH} - \beta P\left(\alpha_L, \hat{x}_{HH}\right) L\right]\} \\
= \;& P_H\left[(1+\beta) P\left(\alpha_H, \hat{x}_{HH}\right) L + \hat{x}_{HH} - (1+\beta) P\left(\alpha_H, \hat{x}_{LH}\right) L - \hat{x}_{LH}\right] \\
& + P_L \beta L\{P\left(\alpha_L, \hat{x}_{LL}\right) + (1-q)\left[P\left(\alpha_H, \hat{x}_{LH}\right) - P\left(\alpha_L, \hat{x}_{LH}\right)\right] \\
& - P\left(\alpha_L, \hat{x}_{HL}\right) - (1-q)\left[P\left(\alpha_H, \hat{x}_{HH}\right) - P\left(\alpha_L, \hat{x}_{HH}\right)\right]\} \\
= \;& P_H\left[(1+\beta) P\left(\alpha_H, \hat{x}_{HH}\right) L + \hat{x}_{HH} - (1+\beta) P\left(\alpha_H, \hat{x}_{LH}\right) L - \hat{x}_{LH}\right] \\
& + P_L \beta L\,(1-q)\left[P\left(\alpha_H, \hat{x}_{LH}\right) - P\left(\alpha_L, \hat{x}_{LH}\right) - P\left(\alpha_H, \hat{x}_{HH}\right) + P\left(\alpha_L, \hat{x}_{HH}\right)\right].
\end{aligned}$$

Take partial derivative of above express with respect to q,

$$\begin{aligned}
\frac{\partial^2 C}{\partial \xi \partial q} &= P_H \left\{ \left[(1+\beta) P_x \left(\alpha_H, \hat{x}_{HH} \right) L + 1 \right] \frac{\partial \hat{x}_{HH}}{\partial q} \right. \\
&\quad \left. - \left[(1+\beta) P_x \left(\alpha_H, \hat{x}_{LH} \right) L + 1 \right] \frac{\partial \hat{x}_{LH}}{\partial q} \right\} \\
&\quad + P_L \beta L (1-q) \left\{ \left[P_x \left(\alpha_H, \hat{x}_{LH} \right) - P_x \left(\alpha_L, \hat{x}_{LH} \right) \right] \frac{\partial \hat{x}_{LH}}{\partial q} \right. \\
&\quad \left. - \left[P_x \left(\alpha_H, \hat{x}_{HH} \right) - P_x \left(\alpha_L, \hat{x}_{HH} \right) \right] \frac{\partial \hat{x}_{HH}}{\partial q} \right\} \\
&= P_H \frac{\partial \hat{x}_{HH}}{\partial q} \{ \left[(1+\beta) P_x \left(\alpha_H, \hat{x}_{HH} \right) L + 1 \right] \\
&\quad - \frac{P_L}{P_H} \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{HH} \right) - P_x \left(\alpha_L, \hat{x}_{HH} \right) \right] \} \\
&\quad - P_H \frac{\partial \hat{x}_{LH}}{\partial q} \{ \left[(1+\beta) P_x \left(\alpha_H, \hat{x}_{LH} \right) L + 1 \right] \\
&\quad - \frac{P_L}{P_H} \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{LH} \right) - P_x \left(\alpha_L, \hat{x}_{LH} \right) \right] \}
\end{aligned}$$

From equations (6.3) and (6.7), it follows

$$\begin{aligned}
\frac{\partial^2 C}{\partial \xi \partial q} &= P_H \frac{\partial \hat{x}_{HH}}{\partial q} \left\{ - \frac{(1-\xi) P_L}{\xi P_H} \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{HH} \right) - P_x \left(\alpha_L, \hat{x}_{HH} \right) \right] \right. \\
&\quad \left. - \frac{P_L}{P_H} \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{HH} \right) - P_x \left(\alpha_L, \hat{x}_{HH} \right) \right] \right\} \\
&\quad - P_H \frac{\partial \hat{x}_{LH}}{\partial q} \left\{ - \frac{\xi P_L}{(1-\xi) P_H} \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{LH} \right) - P_x \left(\alpha_L, \hat{x}_{LH} \right) \right] \right. \\
&\quad \left. - \frac{P_L}{P_H} \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{LH} \right) - P_x \left(\alpha_L, \hat{x}_{LH} \right) \right] \right\} \\
&= - P_H \frac{\partial \hat{x}_{HH}}{\partial q} \frac{P_L}{P_H} \left[\frac{(1-\xi)}{\xi} + 1 \right] \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{HH} \right) - P_x \left(\alpha_L, \hat{x}_{HH} \right) \right] \\
&\quad + P_H \frac{\partial \hat{x}_{LH}}{\partial q} \frac{P_L}{P_H} \left[\frac{\xi}{(1-\xi)} + 1 \right] \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{LH} \right) - P_x \left(\alpha_L, \hat{x}_{LH} \right) \right].
\end{aligned}$$

Rearranging the above expression,

$$\begin{aligned}
\frac{\partial^2 C}{\partial \xi \partial q} &= - P_L \frac{\partial \hat{x}_{HH}}{\partial q} \frac{1}{\xi} \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{HH} \right) - P_x \left(\alpha_L, \hat{x}_{HH} \right) \right] \\
&\quad + P_L \frac{\partial \hat{x}_{LH}}{\partial q} \frac{1}{1-\xi} \beta L (1-q) \left[P_x \left(\alpha_H, \hat{x}_{LH} \right) - P_x \left(\alpha_L, \hat{x}_{LH} \right) \right]. \quad (6.17)
\end{aligned}$$

From first order condition (6.3),

$$\begin{aligned}
&\frac{\partial \hat{x}_{HH}}{\partial q} \\
= \; & \frac{\frac{(1-\xi)P_L}{\xi P_H}\left[P_x\left(\alpha_H, \hat{x}_{HH}\right) - P_x\left(\alpha_L, \hat{x}_{HH}\right)\right]}{\left(1+\frac{1}{\beta}\right)P_{xx}\left(\alpha_H, \hat{x}_{HH}\right) + \frac{(1-\xi)P_L}{\xi P_H}(1-q)\left[P_{xx}\left(\alpha_H, \hat{x}_{HH}\right) - P_{xx}\left(\alpha_L, \hat{x}_{HH}\right)\right]}.
\end{aligned}$$

Similarly, from first order condition (6.9),

$$\begin{aligned}
&\frac{\partial \hat{x}_{LH}}{\partial q} \\
= \; & \frac{\frac{\xi P_L}{(1-\xi)P_H}\left[P_x\left(\alpha_H, \hat{x}_{LH}\right) - P_x\left(\alpha_L, \hat{x}_{LH}\right)\right]}{\left(1+\frac{1}{\beta}\right)P_{xx}\left(\alpha_H, \hat{x}_{LH}\right) + \frac{\xi P_L}{(1-\xi)P_H}(1-q)\left[P_{xx}\left(\alpha_H, \hat{x}_{LH}\right) - P_{xx}\left(\alpha_L, \hat{x}_{LH}\right)\right]}.
\end{aligned}$$

If $P(\alpha, x)$ satisfies (2.26), note that

$$P_{xx}(\alpha, x) > 0, \; P_x\left(\alpha_H, x\right) - P_x\left(\alpha_L, x\right) < 0,$$

it follows that

$$\begin{aligned}
\frac{\partial^2 C}{\partial \xi \partial q} \; \geq \; & \left\{-P_L \frac{\partial \hat{x}_{HH}}{\partial q}\frac{1}{\xi}\beta L(1-q)\left[\left(-P_{xx}\left(\alpha_H, \hat{x}_{HH}\right)\right]\right.\right. \\
& \left.\left. + P_L \frac{\partial \hat{x}_{LH}}{\partial q}\frac{1}{1-\xi}\beta L(1-q)\left[-P_{xx}\left(\alpha_H, \hat{x}_{LH}\right)\right]\right\}\right. \\
& \cdot\left[-\frac{P_x\left(\alpha_H, \hat{x}_{HH}\right) - P_x\left(\alpha_L, \hat{x}_{HH}\right)}{P_{xx}\left(\alpha_H, \hat{x}_{HH}\right)}\right].
\end{aligned}$$

However,

$$\begin{aligned}
& P_L \frac{\partial \hat{x}_{HH}}{\partial q} P_{xx}\left(\alpha_H, \hat{x}_{HH}\right)\frac{1}{\xi}\beta L(1-q) \\
= \; & \frac{\frac{(1-\xi)P_L}{\xi P_H}\left[P_x\left(\alpha_H, \hat{x}_{HH}\right) - P_x\left(\alpha_L, \hat{x}_{HH}\right)\right]}{\xi\left(1+\frac{1}{\beta}\right) + \frac{(1-\xi)P_L}{P_H}(1-q)\left[1 - \frac{P_{xx}(\alpha_L, \hat{x}_{HH})}{P_{xx}(\alpha_H, \hat{x}_{HH})}\right]}\beta L(1-q)P_L \\
= \; & -\frac{(1+\beta)P_x(\alpha_H, \hat{x}_{HH}) + 1}{\xi\left(1+\frac{1}{\beta}\right) + \frac{(1-\xi)P_L}{P_H}(1-q)\left[1 - \frac{P_{xx}(\alpha_L, \hat{x}_{HH})}{P_{xx}(\alpha_H, \hat{x}_{HH})}\right]}\beta L(1-q)P_L,
\end{aligned}$$

$$P_L \frac{\partial \hat{x}_{LH}}{\partial q} P_{xx}\left(\alpha_H, \hat{x}_{LH}\right)\frac{1}{1-\xi}\beta L(1-q)$$

$$
\begin{aligned}
&= \frac{\frac{\xi P_L}{(1-\xi)P_H}\left[P_x\left(\alpha_H,\hat{x}_{LH}\right)-P_x\left(\alpha_L,\hat{x}_{LH}\right)\right]}{(1-\xi)\left(1+\frac{1}{\beta}\right)+\frac{\xi P_L}{P_H}(1-q)\left[1-\frac{P_{xx}(\alpha_L,\hat{x}_{LH})}{P_{xx}(\alpha_H,\hat{x}_{LH})}\right]}\beta L\left(1-q\right)P_L \\
&= -\frac{(1+\beta)P_x\left(\alpha_H,\hat{x}_{LH}\right)+1}{(1-\xi)\left(1+\frac{1}{\beta}\right)+\frac{\xi P_L}{P_H}(1-q)\left[1-\frac{P_{xx}(\alpha_L,\hat{x}_{LH})}{P_{xx}(\alpha_H,\hat{x}_{LH})}\right]}\beta L\left(1-q\right)P_L,
\end{aligned}
$$

and

$$
(1+\beta)P_x\left(\alpha_H,\hat{x}_{LH}\right)+1 \geq (1+\beta)P_x(\alpha_H,\hat{x}_{HH})+1 \geq 0
$$

since $\beta \ll 1$, it follows that

$$
\begin{aligned}
& -P_L\frac{\partial \hat{x}_{LH}}{\partial q}P_{xx}\left(\alpha_H,\hat{x}_{LH}\right)\frac{1}{1-\xi}\beta L\left(1-q\right) \\
& +P_L\frac{\partial \hat{x}_{HH}}{\partial q}P_{xx}\left(\alpha_H,\hat{x}_{HH}\right)\frac{1}{\xi}\beta L\left(1-q\right) \\
> \;& 0,
\end{aligned}
$$

i.e.,

$$
\frac{\partial^2 C}{\partial \xi \partial q} \geq 0.
$$

If $P(\alpha,x)$ satisfies (2.25)

$$
\begin{aligned}
& \frac{\partial \hat{x}_{LH}}{\partial q}\frac{1}{(1-\xi)}\left[P_x\left(\alpha_H,\hat{x}_{LH}\right)-P_x\left(\alpha_L,\hat{x}_{LH}\right)\right] \\
& -\frac{\partial \hat{x}_{HH}}{\partial q}\frac{1}{\xi}\left[P_x\left(\alpha_H,\hat{x}_{HH}\right)-P_x\left(\alpha_L,\hat{x}_{HH}\right)\right] \\
= \;& \left(P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L)\right)\left[\frac{\partial \hat{x}_{LH}}{\partial q}\frac{1}{1-\xi}P_x^{(2)}(\hat{x}_{LH})-\frac{\partial \hat{x}_{HH}}{\partial q}\frac{1}{\xi}P_x^{(2)}\left(\hat{x}_{HH}\right)\right],
\end{aligned}
$$

then in order to show

$$
\frac{\partial^2 C}{\partial \xi \partial q} \geq 0,
$$

it only needs to show

$$
\frac{\partial \hat{x}_{LH}}{\partial q}\frac{1}{1-\xi}P_x^{(2)}(\hat{x}_{LH})-\frac{\partial \hat{x}_{HH}}{\partial q}\frac{1}{\xi}P_x^{(2)}\left(\hat{x}_{HH}\right) \geq 0.
$$

But

$$\begin{aligned}
&\frac{\partial \hat{x}_{LH}}{\partial q}\frac{1}{1-\xi}P_x^{(2)}(\hat{x}_{LH}) \\
= \;& \frac{\frac{\xi P_L}{(1-\xi)P_H}\left[P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L)\right]P_x^{(2)}(\hat{x}_{LH})\frac{1}{1-\xi}P_x^{(2)}(\hat{x}_{LH})}{\left(1+\frac{1}{\beta}\right)P^{(1)}(\alpha_H)P_{xx}^{(2)}(\hat{x}_{LH})+\frac{\xi P_L(1-q)}{(1-\xi)P_H}(P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L))P_{xx}^{(2)}(\hat{x}_{LH})},
\end{aligned}$$

and from first order condition (6.7)

$$\begin{aligned}
&P_x^{(2)}(\hat{x}_{LH}) \\
= \;& -\left[(1+\beta)\,P^{(1)}(\alpha_H)L+(1-q)\,\frac{\xi P_L}{(1-\xi)\,P_H}\beta L(P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L))\right]^{-1},
\end{aligned}$$

similarly,

$$\begin{aligned}
&\frac{\partial \hat{x}_{HH}}{\partial q}\frac{1}{\xi}P_x^{(2)}(\hat{x}_{HH}) \\
= \;& \frac{\frac{(1-\xi)P_L}{\xi P_H}\left[P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L)\right]P_x^{(2)}(\hat{x}_{HH})\frac{1}{\xi}P_x^{(2)}(\hat{x}_{HH})}{\left(1+\frac{1}{\beta}\right)P^{(1)}(\alpha_H)P_{xx}^{(2)}(\hat{x}_{HH})+\frac{(1-\xi)P_L(1-q)}{\xi P_H}(P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L))P_{xx}^{(2)}(\hat{x}_{HH})},
\end{aligned}$$

and

$$\begin{aligned}
&P_x^{(2)}(\hat{x}_{HH}) \\
= \;& -\left[(1+\beta)\,P^{(1)}(\alpha_H)L+(1-q)\,\frac{(1-\xi)P_L}{\xi P_H}\beta L(P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L))\right]^{-1}.
\end{aligned}$$

Since $P_{xx}^{(2)}(x)$ is a monotone function of x, from the fact that

$$\lim_{x\to\infty} P(\alpha,x)=0,$$

it can easily show $P_{xx}^{(2)}(x)$ is a non increasing function of x, then again since $\beta \ll 1$,

$$\begin{aligned}
&\frac{-\frac{1}{1-\xi}P_x^{(2)}(\hat{x}_{LH})}{\left(1+\frac{1}{\beta}\right)P^{(1)}(\alpha_H)P_{xx}^{(2)}(\hat{x}_{LH})+\frac{\xi P_L(1-q)}{(1-\xi)P_H}(P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L))P_{xx}^{(2)}(\hat{x}_{LH})} \\
> \;& \frac{-\frac{1}{\xi}P_x^{(2)}(\hat{x}_{HH})}{\left(1+\frac{1}{\beta}\right)P^{(1)}(\alpha_H)P_{xx}^{(2)}(\hat{x}_{HH})+\frac{(1-\xi)P_L(1-q)}{\xi P_H}(P^{(1)}(\alpha_H)-P^{(1)}(\alpha_L))P_{xx}^{(2)}(\hat{x}_{HH})},
\end{aligned}$$

so in order to show

$$\frac{\partial^2 C}{\partial \xi \partial q} \geq 0,$$

it only needs to show

$$\begin{aligned} & -\frac{\xi P_L}{(1-\xi) P_H}\left[P^{(1)}(\alpha_H) - P^{(1)}(\alpha_L)\right] P_x^{(2)}(\hat{x}_{LH}) \\ \geq & -\frac{(1-\xi) P_L}{\xi P_H}\left[P^{(1)}(\alpha_H) - P^{(1)}(\alpha_L)\right] P_x^{(2)}(\hat{x}_{HH}), \end{aligned}$$

from first order conditions (6.3) and (6.7) and the fact that $P_{xx}(\alpha, x) > 0$, the desired result follows.

6.4 Convexity of Benefit of Security Audits

Recall that

$$\frac{\partial C_H}{\partial q} = -\frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}\left(\hat{S}_{HH} - \beta P(\alpha_L, \hat{x}_{HH}) L\right),$$

thus the second derivative of benefit of security audits with respect to audit intensity when the principal observes $\eta = \alpha_H$ is

$$\begin{aligned} -\frac{\partial^2 C_H}{\partial q^2} &= \partial\left[\frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L}\left(\hat{S}_{HH} - \beta P(\alpha_L, \hat{x}_{HH}) L\right)\right] / \partial q \\ &= \frac{(1-\xi) P_L}{\xi P_H + (1-\xi) P_L} \frac{\partial\left(\hat{S}_{HH} - \beta P(\alpha_L, \hat{x}_{HH}) L\right)}{\partial q}, \end{aligned}$$

where

$$\hat{S}_{HH} = \beta P(\alpha_L, \hat{x}_{HH}) L,$$

hence

$$\begin{aligned} -\frac{\partial^2 C_H}{\partial q^2} &= \frac{(1-\xi) P_L \beta L}{\xi P_H + (1-\xi) P_L} \frac{\partial\left[P(\alpha_H, \hat{x}_{HH}) - P(\alpha_L, \hat{x}_{HH})\right]}{\partial q} \\ &= \frac{(1-\xi) P_L \beta L\left[P_x(\alpha_H, \hat{x}_{HH}) - P_x(\alpha_L, \hat{x}_{HH})\right]}{\xi P_H + (1-\xi) P_L} \cdot \frac{\partial \hat{x}_{HH}}{\partial q}. \end{aligned}$$

From equation 6.3, it follows that

$$\begin{aligned}
&\frac{\partial \hat{x}_{HH}}{\partial q} \\
= \; & \frac{\frac{(1-\xi)P_L}{\xi P_H}\beta L\left[P_x\left(\alpha_H, \hat{x}_{HH}\right) - P_x\left(\alpha_L, \hat{x}_{HH}\right)\right]}{\left(1+\beta\right)P_{xx}\left(\alpha_H, \hat{x}_{HH}\right)L + \left(1-q\right)\frac{(1-\xi)P_L}{\xi P_H}\beta L\left[P_{xx}\left(\alpha_H, \hat{x}_{HH}\right) - P_{xx}\left(\alpha_L, \hat{x}_{HH}\right)\right]} \\
> \; & 0.
\end{aligned}$$

Therefore,

$$-\frac{\partial^2 C_H}{\partial q^2} > 0.$$

Similarly, it can be shown that

$$-\frac{\partial^2 C_L}{\partial q^2} > 0.$$

6.4.1 Proof of Proposition 8

If

$$\frac{\partial C_H/\partial q}{\partial C_L/\partial q}|_{q=0} > 1,$$

it means the that marginal benefit of a security audit is greater when the principal observes $\eta = \alpha_H$ than when the principal observes $\eta = \alpha_L$. Thus the principal has the incentive to pre-commit to a more intensive security audit when she observes $\eta = \alpha_H$. However, this is not always the case, a numerical counter example is presented below.

Let

$$\begin{aligned}
P\left(\alpha, x\right) &= \frac{\alpha}{1+x}, \\
\alpha_H &= 0.7, \\
\alpha_L &= 0.4, \\
L &= 1000,
\end{aligned}$$

$$\begin{aligned}\beta &= 0.1,\\ \xi &= 2/3.\end{aligned}$$

It can easily be shown that when

$$\frac{P_L}{P_H} = 3,$$

$$\frac{\partial C_H/\partial q}{\partial C_L/\partial q}|_{q=0} = 1.08;$$

however, if

$$\frac{P_L}{P_H} = 2,$$

then

$$\frac{\partial C_H/\partial q}{\partial C_L/\partial q}|_{q=0} = 0.92.$$

Thus, the principal does not always pre-commit to a more intensive security audit when she observes $\eta = \alpha_H$.

BIBLIOGRAPHY

[1] Antle, R. and G. D. Eppen, "Capital Rationing and Organizational Slack in Capital Budgeting," *Management Science*, Vol. 31, No. 2 (February 1985), pp. 163-174.

[2] Arrow, Kenneth J., "The Economics of Agency," in *Principals and Agents: The Structure of Business*, John W. Patt and Richard J. Zeckhouser (eds.) Harvard Business School Press, Boston, MA (1985), pp. 37-53.

[3] Ball, R., "Anomalies in Relationships between Securities' Yields and Yield-Surrogates," *Journal of Financial Economics*, Vol. 6 (1978), pp. 103-126.

[4] Banz, R. W., "The Relationship between Return and Market Value of Common Stocks," *Journal of Financial Economics*, Vol. 9 (1981), pp. 3-18.

[5] Baiman, S., "Agency Research in Managerial Accounting: A Second Look," *Accounting, Organizations and Society*, Vol. 15, No. 4 (1990), pp. 341-371.

[6] Baiman, S. and J. Demski, "Economically Optimal Evaluation and Control Systems," *Journal of Accounting Research* (Supplement 1980), pp. 184-220.

[7] Baiman, S. and J. H. Evans III, "Pre-Decision Information and Participative Management Control Systems," *Journal of Accounting Research*, Vol. 21, No. 2 (Autumn 1983), pp. 371-395.

[8] Baron, D. P. and D. Besanko, "Regulation, Asymmetric Information, and Auditing," *Rand Journal of Economics*, Vol. 15, No. 4 (Winter 1984), pp. 447-470.

[9] Basu, S., "The Relationship between Earnings Yield, Market Value, and Return for NYSE Common Stocks: Further Evidence," *Journal of Financial Economics*, Vol. 12 (1983), pp. 129-156.

[10] Bhandari, L. C., "Debt/Equity Ratio and Expected Common Stock Returns: Empirical Evidence," *Journal of Finance*, Vol. 43 (1988), pp. 507-528.

[11] Campbell, K., L. A. Gordon, M. P. Loeb and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security*, Vol. 11 (2003), pp. 431-448.

[12] Cavusoglu, H., M. Birendra and S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers," University of Texas at Dallas, working paper (2002).

[13] Dye, R., "Optimal Monitoring Policies in Agencies," *The Rand Journal of Economics*, Vol. 17, No. 3 (Autumn 1986), pp. 339-350.

[14] Gordon, L. A. and M. P. Loeb, "A Framework for Using Information Security as a Response to Competitor Analysis Systems," *Communications of the ACM* (September 2001), pp. 70-75.

[15] Ettredge, M. and V. J. Richardson, "Assessing the Risk in E-Commerce," *Proceedings of the 35th Hawaii International Conference on System Sciences (2002).*

[16] Fama, E. F. and K. R. French, "Multifactor Explanations of Asset Pricing Anomalies," *Journal of Finance*, Vol. LI, No. 1 (March 1996), pp. 55-84.

[17] Fama, E. F. and K. R. French, "Common Risk Factors in the Returns on Stocks and Bonds," *Journal of Financial Economics*, Vol. 33 (1993), pp. 3-56.

[18] Fama, E. F. and K. R. French, "The Cross-Section of Expected Stock Returns," *Journal of Finance*, Vol. XLVII, No. 2 (June 1992), pp. 427-465.

[19] Garg, A., J. Curtis and H. Halper, "Quantifying the Financial Impact of IT Security Breaches," *Information Management & Computer Security*, Vol. 11, No. 2 (2003), pp. 74-83.

[20] Gordon, L. A. and M. P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, (November 2002), pp. 438-457.

[21] Gordon, L. A. and K. J. Smith, "Postauditing Capital Expenditures and Firm Performance: The Role of Asymmetric Information," *Accounting, Organizations and Society*, Vol. 17, No. 8 (1992), pp. 741-757.

[22] Gulliver, F. R., "Post-project appraisal pay," *Harvard Business Review,* (March-April 1987) pp. 128-130.

[23] Holmstrom, B., "Moral Hazard and Observability," *The Bell Journal of Economics*, (1979), pp. 74-91.

[24] Harris, M., C. H. Kriebel and A. Raviv, "Asymmetric Information, Incentives and Intrafirm Resource Allocation," *Management Science*, Vol. 28, No. 6 (Jun 1982), pp. 604-620.

[25] Harris, M. and A. Raviv, "The Capital Budgeting Process: Incentives and Information," *The Journal of Finance*, Vol. LI, No. 4 (September 1996), pp. 1139-1174.

[26] Khalil, F., "Auditing without Commitment," *The Rand Journal of Economics*, Vol. 28, No. 4 (Winter 1997), pp. 629-640.

[27] Kim, S. K. and Y. S. Suh, "Conditional Monitoring Policy under Moral Hazard," *Management Science*, Vol. 38, No. 8 (August 1992), pp. 1106-1120.

[28] Lintner, J., "The Valuation of Risk Assets and the Selection of Risky Investments in Stock Portfolios and Capital Budgets," *Review of Economics and Statistics*, Vol. 47 (1965), pp. 13-37.

[29] Myers, M. D., L. A. Gordon and M. M. Hamer, "Postauditing Capital Assets and Firm Performance: an Empirical Investigation," *Managerial and Decision Economics,* (August 1991) pp. 317-327.

[30] Myerson, R. B., "Incentive Compatibility and The Bargaining Problem," *Econometrica*, Vol. 47, No. 1 (January 1979), pp. 61-73.

[31] Ng, D. S. and J. Stoeckenius, "Auditing: Incentives and Truthful Reporting," *Journal of Accounting Research*, Vol. 17, Studies on Auditing-Selections from the "Research Opportunities in Auditing" Program, (1979), pp. 1-24.

[32] Penno, M., "Asymmetry of Pre-Decision Information and Managerial Accounting," *Journal of Accounting Research*, Vol. 22, No. 1 (Spring 1984), pp. 177-191.

[33] Power, R., "CSI/FBI 2002 Computer Crime and Security Survey," *Computer Security Issues & Trends*, Vol. 18, No. 2 (2002), pp. 7-30.

[34] Richardson, R., "2003 CSI/FBI Computer Crime and Security Survey," *Computer Security Journal*, XIX(2) (2003), pp. 21-40.

[35] Rosenberg, B., K. Reid and R. Lanstein, "Persuasive Evidence of Market Inefficiency," *Journal of Portfolio Management*, Vol. 11 (1985), pp. 9-17.

[36] Sharpe, W. F., "Capital Asset Prices: A Theory of Market Equilibrium under Conditions of Risk," *Journal of Finance*, Vol. 19 (1964), pp. 425-442.

[37] Stattman, D., "Book Values and Stock Returns," *The Chicago MBA: A Journal of Selected Papers*, Vol. 4 (1980), pp. 25-45.