December 2002

THE ECONOMICS OF INFORMATION TECHNOLOGY (IT) SECURITY

Huseyin Cavusoglu
The Univesity of Texas at Dallas

THE ECONOMICS OF INFORMATION TECHNOLOGY (IT) SECURITY

Huseyin Cavusoglu
The Univesity of Texas at Dallas
huseyin@utdallas.edu

Abstract

IT Security has become a salient issue for many organizations. While the literature on the technical aspects of IT security is proliferating, it is not clear how one can quantify the value of IT security. An assessment of the value of IT security technology is critical both to firms employing this technology as well as to firms that develop the technology. However assessing the value of IT security is a challenging task because of difficulties in measurements of tangible and intangible benefits of it. My thesis addresses the broad issue of the value of IT security. I use both analytical and empirical methodologies. In the first part of my thesis, I conduct an event study analysis of the effect of security breach announcements on market value of firms. This analysis provides an indirect estimate of the costs of inadequate IT security. In the second and third parts of my thesis, I consider a typical IT security architecture that includes preventive, detective, and response security controls. I develop a game theoretical model that incorporates the strategic interaction between a firm that invests in IT security and users of the system. I derive the value of IT security mechanisms as the savings in organizational loss because of security technology. I also plan to analyze the optimal investments in various technologies. My research will yield guidelines and insights that will help firms decide their security architectures and security developers make their design decisions.

Problem Statement

Increased interconnectivity among computers enabled by networking technologies, in particular the Internet, has boosted the scale and scope of information technology (IT) related crimes. Open access nature of the Internet that assists easy exchange of ideas, goods, and services also presents the biggest impediment to its lasting success in the form of security. The cost of a single security breach can be enormous in terms of monetary damage, corporate liability and credibility.

The laws and regulations enacted by government act as a broad deterrent against IT-related crime. These "external control" mechanisms reinforce the security management within the firm or "internal control". IT security, which was once considered an overhead to a company's main operation, is now widely recognized as an important aspect of business operations (Cagnemi 2001). Security of IT systems is no longer purely the concern of the traditional high-risk category organizations such as those in the defense, military, or government sectors. While high-risk organizations may adopt security at any price, most commercial environments will have to balance the benefits against the costs of security technologies employed by efficient management of IT security.

Despite the economic importance of IT security to organizations, very little academic research has been devoted to analyze the issue from an economic perspective. While the literature on the technical aspects of IT security is proliferating, it is not clear how one can quantify as well as identify the drivers of IT security. An assessment of the value of the IT security technology is critical to both firms employing this technology as well as firms that develop the technology. I seek to understand the economic value of different components of IT security architecture and the drivers of the value in order to provide normative guidelines to decision makers in the IT security domain.

Research Questions

The context of IT security management offers a rich set of problems for academic research. From an economics perspective, quantifying the value of IT security is complex because of the difficulties in estimating costs and benefits. However, any insight into the relative contribution of various security mechanisms is very useful to both IT security developers and deployers. Consequently, the problem requires investigation from multiple perspectives. My thesis addresses the broad issue of value of IT security. I use analytical modeling and empirical analysis methodologies to assess the value of IT security. In the analytical modeling methods, I use a model of IT security architecture that consists of multiple layers with different capabilities and characteristics. The value of a security mechanism at any level depends critically on the structures and capabilities of mechanisms surrounding it. Many of the IT security mechanisms are also IT-based and are often imprecise leading to false-positive and false-negative signals from these security systems. The cost structures associated with security mechanisms at different levels can be sharply different, necessitating simultaneous design of all layers of security control.

Using a model that captures the above essential aspects of IT architecture, I derive the value of different components of this architecture to firms that deploy them. If the parameters of the model can be estimated, then the value can be estimated. I call this is the "direct" approach to value assessment. In the second method, I assess the value of IT security by determining the loss in market value because of security breach incidents. The assumption here is that the investors can assess the impact of security breaches and those assessments are reflected in stock prices. I call this the "indirect" approach to value assessment. I describe the specifics of these methods below.

The Effect of Internet Security Breach Announcements on Capital Markets

The insurance notion of IT security coupled with the fact that the net present value analysis of the direct cost of security breaches, which grossly under estimates the cost of security breach, has lead corporate managers to under invest in IT security. Even when corporate managers view information security as a value creator and understand the indirect costs of security breaches, it is difficult for them to quantify the cost of security breaches as most costs are soft or intangible. Though a direct way of measuring these costs seems quite difficult, an indirect estimate of these costs can be made through capital markets. In this research, I address the following questions

1. Do security breaches affect the market value of firms? What are the factors that determine the size of the reaction?
2. Is there any 'information transfer' of security breach announcements to internet security product developers? Namely, do investors reward the firms that are likely to gain from security breaches?

Methodology

In my first research I address first and second questions using an empirical approach. I employ widely-accepted event study methodology to assess the impact of Internet security breaches on the market value of the breached firms. In addition, I study the information transfer effect of security breaches, namely the effect of security breaches of disclosing firms on market values of Internet security firms. Using the efficient market hypothesis, I study (i) whether the investors penalize the firm for security breaches and to what extent the indirect costs are impounded in the firm value and (ii) to what extent investors reward the firms that are likely to gain from the security breaches by selling more security related hardware and software.

In efficient markets, rational investors are assumed to impound all publicly available information available to that date on the expected future cash flows of the firm and discount them appropriately to reach the current firm value. Thus I expect that investors will recognize both current and future implications of security breaches on the expected future cash flows of the firm and will adjust the firm value accordingly. It has been well documented in information transfer literature that investor not only use information released by a firm to evaluate its stock price they also use this information to revise their beliefs about the stock price of related firms. Thus the disclosure of security breach by the affected firm may result in the price revision of Internet security developers that may likely to gain form additional demand from security products.

Preliminary Findings

The results of my analysis show that announcements of Internet security breaches are negatively associated with the market value of announcing firms. Compromised firms, on the average, lose around 2.1% of their market values within two days surrounding the events. In addition my results suggest that the effects of security breaches are not restricted to breached firms. The market

values of security developers increase, on the average, 1.3% per security breach announcement. Overall, my study shows that investors pay attention to news concerning Internet security breaches. The findings that average (negative) cumulative abnormal return (CAR) associated with announcements decreases with the size of the firm suggest that smaller firms are penalized more than large firms by investors when a security breach occurs. This result has several implications. For the managers of small firms, this study serves as a reminder of the importance of security for survivability of these firms. They should start to see the security not only as a risk-reducer but also as an enabler in this internetworked world. An emerging solution is to buy insurance in order not to be affected severely in case of a breach. This can pay for the third party liability but cannot get back the lost consumer confidence. The effectiveness of such insurance as risk management tool require more in depth analysis by both IS researchers and firms and is an important avenue for future research.

Although, market penalizes all firms for security breaches, net firms are penalized more compared to conventional firms. A possible explanation for this effect is the differential degree of dependency by the firms on Internet to generate revenues. Firms that solely depend on the Internet as a revenue generating mechanism pay higher prices in case of a security breach than the firms that have multiple channels to exploit. Security of IT systems for net firms is utmost important for their success. The implication for the management is to view information security as an enabler of value creation rather than a risk avoidance measure.

Further I show that negative effects of security problem have risen over time. The consequences of security breaches are much higher for new incidents. In the face of decreasing cost of security products in response to drop in cost of technology and rising vulnerabilities of systems as a result of greater dependency on technology, the risk of a security breach should be periodically reassessed by the management and necessary step should be taken to mitigate the risk. This requires seeing the security as a process that begins with *assessment* followed by *policy*, *implementation*, *training* and *testing* (Maiwald 2000).

The finding that the firms experience similar CARs irrespective of the nature of attack is quite interesting. One possible explanation is that investors regard any kind of security breach as failure of IT security of firms and penalize them for not having taken essential steps to prevent security problems. This shows that availability, although very important in e-commerce, is not the only criterion that determines the market's response to a security breach. I couldn't classify the attacks into more than two categories because I didn't have enough observations. This issue requires further investigation. Future research should focus on more general classification of attack types on a larger data set.

The finding that security firms realize significant positive returns as a reaction to announcements on security breaches justifies that security and e-commerce go hand in hand. You cannot have e-commerce without security. The general rise in stock prices of Internet security firms further justifies this argument because security can be improved only with a series of security controls. Investors turn to the shares of Internet security firms with the belief that the computer crimes will step up demand for these stocks.

My results show that the true cost of security is not restricted to cost of replacing the breached systems. The cost due to loss of market capitalization may be more devastating than the direct cost of breach. All companies should be concerned about information security issues because it is an issue that has enormous potential to negatively impact the valuation of a company's stock.

The Value of Intrusion Detection Systems (IDS) in IT Security

IT security management seeks to establish internal controls to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorized disclosure of information. These internal mechanisms fall into two major categories: *preventive control* and *detective control*. Preventive control mechanisms, e.g. firewalls, aim to develop a 'defensive shield' around IT systems to secure them. The detective control mechanisms, e.g. Intrusion Detection Systems (IDS), try to detect the intrusions when they occur. Although preventive control constitutes an important aspect of IT security architecture, it is extremely difficult to build an IT system that is absolutely secure. Detection-based security has become an important element in overall security architecture because IT systems are unprotected without detective controls once intruders manage to break the firewall. To that end, I first investigate the value of IDS within an IT security architecture that has firewalls on one side and manual monitoring on the other side surrounding the IDS to answer the questions:

1. What is the value of preventive control (IDS) in IT security architecture of firms?
2. When are the manual inspections required and how should they be implemented? By implementation we mean the frequency of inspections, and budget for random inspections?

Methodology

In my second research, I develop an analytical model to address third and fourth questions. My focus in this research is on the value of IDS given a firewall technology and a manual monitoring process. I derive the value of IDS by comparing two cases. In the first case, I focus on an architecture that doesn't employ IDS to detect intrusions. Manual monitoring of the system log files and audit trials is the only way to detect intrusions in this scenario. In the second case, I examine the situation in which IDS assists in the detection of intrusions. The firm that employs the IDS also uses manual monitoring because the signals from the IDS are imperfect. The objective in both cases is to minimize total organizational loss, which includes the cost of intrusions, both undetected and detected, and the cost of manual monitoring. I analyze the issue from a strategic perspective using a game-theoretic approach that consider hacking activity a rational choice made by hackers. I derive the value of IDS by comparing organizational payoffs with and without IDS.

Preliminary Findings

In addition to proposing normative guidelines to the firms, such as the frequency of monitoring, I am able to characterize conditions where the use of the IDS is beneficial to the firm in terms of reducing the total organizational loss. I find that the value of the IDS depends critically on (i) benefit to cost ratio of intrusion for the hacker, (ii) cost to benefit ratio of monitoring for the firm, and (iii) the false-positive and false-negative rates of the IDS. My analysis reveals that the value of IDS comes not only from improved detection of intrusions but also from increased deterrence to hackers. A surprising result of my analysis is that in some regions of the parameter space, IDS increases the hacking activity, and consequently, the firm located in those regions is better off not employing IDS. Also I find that preventive control mechanisms decrease the need for detective controls such as the IDS. Thus, the firewall can substitute the IDS to some extent. However, tighter firewalls also require substantial investment and may have negative consequences by preventing legitimate users from getting to systems. Thus, firms have to carefully analyze the relative cost of investments for firewall and the IDS mechanisms before deciding on security architecture. I will try to answer this question in my third research (see section 5 below).

A significant insight from my analysis for the IDS developers relates to the pricing and marketing of IDS. The price of IDS, being information goods with negligible marginal production cost, is dependent primarily on their value to firms. Since the value is higher for industries with higher expected damage and industries that attract a high proportion of hackers, IDS developers can realize substantial profits if they can design IDS specifically for these industries by analyzing the intrusion patterns and nature of information assets to be protected.

My results suggest that the IDS developers should improve the quality of the IDS in both dimensions. Although both q_1 (true positive) and q_2 (true negative) have positive effect on the value of IDS to firms, it is important to note that the extents of their effects are not equal. I find that, for firms that find IDS to be beneficial, the marginal increase in value from a unit increase in q_2 is greater than the marginal increase in value from a unit increase in q_1. This result suggests that IDS developers should try to improve q_2 to generate additional revenue from IDS users. On the other hand, while an increase in q_2 doesn't increase the market size (i.e., the number of firms that realize positive value from IDS), an increase in q_1 increases the market size. Thus, IDS developers are faced with a tradeoff between increasing q_1 or q_2. An IDS developer should carefully weigh in the benefits of increasing the market size vis-à-vis the benefits of increasing the value to users who benefit from IDS when designing IDS.

Optimal Investment in IT Security: Simultaneous Design of Security Control Mechanisms

A collection of security controls must be used to meet the challenges of realistic risk in IT environment. Management has to decide what to reasonably invest for security and control in IT and how to balance risk and control investment. Conventional wisdom is that IT based systems are most effectively controlled by security controls. Development of guidelines to answer questions about how to implement an assortment of security controls is crucial for any solution dealing with IT security. Two prominent issues to answer are

1. How should security budget be allocated into different security controls (technical and manual) to minimize the organizational loss? Do the most effective security measures result in minimum cost? If not, what is the optimum level of effectiveness for the firms?

2. What is the impact of relative cost structure of technical and manual controls on the security strategy?

Methodology

In my third research I address fifth and sixth questions using an analytical model that capture multiple level nature of IT security architecture. Namely I consider that IT security architecture is composed of three layers. I have, at the periphery level, firewalls that attempt to prevent intrusions. At the next level, the IDS attempts to detect intrusions. Then, there is manual monitoring. Different from the first research we take all three security controls endogenous. I solve the model to find the optimum level of effectiveness in each security mechanism and associated investments on them.

Preliminary Findings

This research is in work-in progress phase. I am still working on modeling. Hopefully I will answer the questions specified above after solving the model.

Conclusion

Traditionally, IT security has been seen a subject of computer scientists and economic side of it has been ignored. The ones that tried to explain the economic aspects of IT security have not opened up the blackbox around IT security. They have basically considered risk exposure as well as the cost associated with reducing this exposure through various security controls. In contrast to them I take IS as the basis in my thesis. I specifically model the technology deployed within the IT security blackbox. My analysis provides an assessment of direct value of IT security in terms of reducing direct cost of security breaches.

In addition to direct value of IT security, I provide indirect value of IT security by assessing the value loss in capital markets (indirect cost of security breaches) using a statistically valid event study methodology. My empirical analysis shows that implementation of weak security practices does lead to huge loss in capitalization in case of a security breach.

Overall, I believe that my findings will shed light on the importance of IT security for survivability of firms in today's highly competitive global marketplace. My results should be reassuring to the firms that have invested in information security. For the firms that haven't adopted sound security practices yet due to controversy about its value, it should be a source of encouragement to implement it.

Selected References

Cagnemi, M. P., "Top Technology Issues," *Information Systems Control Journal*, 4, 6, 2001.
Maiwald, E., *Network Security: A Beginner's Guide*, Osborne/McGrawHill, Berkeley, CA, 2001.