December 2002

ASSESSING THE VALUE OF DETECTIVE CONTROL IN IT SECURITY

Huseyin Cavusoglu
The Univesity of Texas at Dallas

Birendra Mishra
The Univesity of Texas at Dallas

Srinivasan Raghunathan
The Univesity of Texas at Dallas

ASSESSING THE VALUE OF DETECTIVE CONTROL IN IT SECURITY

Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan
The Univesity of Texas at Dallas
huseyin@utdallas.edu bmishra@utdallas.edu sraghu@utdallas.edu

Abstract

Recently, IT Security has become a salient issue for many organizations. The cost of a single security breach can be enormous in terms of monetary damage, corporate liability and credibility. Firms increasingly deploy firewalls as a preventive control and Intrusion Detection Systems (IDS) as a detective control to protect IT assets. The IDS has been among the fastest growing IT security products for the last few years. While the literature on the technical aspects of IDS is proliferating, it is not clear how one can quantify the magnitude as well as identify the drivers of IDS benefits. In this paper we seek to assess the value of employing an IDS within an organization's IT security architecture. We analyze the issue from a strategic perspective using a game-theoretic approach and derive the value of IDS by comparing the organizational payoffs with and without IDS. Our analysis reveals the value of IDS comes not only from improved detection of intrusions but also from increased deterrence to hackers. The effects of model parameters, related to firm, hacker, and IDS design, on the value of IDS offer valuable guidance to firms that deploy this technology and those that develop them.

Keywords: IT security, security architecture, detective control, preventive control, intrusion detection systems (IDS), game theory

Introduction

Increased interconnectivity among computers enabled by networking technologies, in particular the Internet, has boosted the scale and scope of information technology (IT) related crimes. As the E-Commerce continues to grow, so does the cyber crime. The DOJ caseload itself reflects the growth of cyber crime. The number of computer intrusion cases jumped from 547 in year 1998 to 1154 in 1999. The losses from computer crime incidents are also rising. Computer Security Institute and FBI 2002 survey found that firms lost $456 million in 2002 in contrast to $378 million in 2001, $266 million in 2000 and $124 million in 1999 (Power 2002).

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. 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 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. Thus, detection based systems complement the perimeter security by identifying intrusions from both insiders and outsiders.

Intrusion Detection Systems (IDS) are one of the most common detection approaches used by firms. The goal of these systems is to identify, in real time, unauthorized use, misuse, or abuse of computer systems. They give warning signals when they detect something suspicious, anomalous, or illegal. Since the signal is not perfect, manual monitoring of log files and audit trails is required to distinguish true alarms from false ones. In addition, manual monitoring is necessary to identify the type of attack the system is under, thereby making it possible to take actions to minimize the damage that could be inflicted on systems.

Despite the economic importance of IT security to organizations, very little academic research has been devoted to analyze the issue from an economic perspective. Most of the academic research on IT security has focused on security technology, such as the development of algorithms for use in the IDS. 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. We 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. To that end, we first investigate the value of IDS within an IT architecture that has firewalls on one side and manual monitoring on the other side surrounding the IDS. We believe that ours is the first study that investigates the IT security architecture from an economic standpoint.

We derive the value of IDS by comparing two cases. In the first case, we 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, we examine the situation in which an 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. In addition to proposing normative guidelines to the firms, such as the frequency of monitoring, we are able to characterize conditions where the use of the IDS is beneficial to the firm in terms of reducing the total organizational loss. We 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. The positive value of IDS is the result of better detection of intrusions and increased deterrence to hackers by IDS. A surprising result of our 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. We also derive valuable insights about the impact of IDS design parameters for IDS developers.

Intrusion Detection Systems

An intrusion in the IT security context can be defined as "any set of actions that attempts to compromise the confidentiality, integrity and availability of a resource" (Lodin 1999). Intrusion detection systems are software and/or hardware systems that automate the process of monitoring the events occurring in computer systems or network segments, and analyze them for signs of intrusions. In recent years, IDS have been accepted as the major tool for the detection of attacks when the perimeter security is breached or when an internal user initiates the attacks. According to International Data Corp. (IDC), the market for the IDS has grown from about $20 million in 1997 to $100 million in 1999 and is projected to reach $528 million by 2005 (Messmer 1999).

An IDS uses audit trails and network packets to detect intrusions. Audit trails store patterns of access to individual objects and histories of events and individuals (National Computer Security Center 1988). Audit trails store information such as date and time of the event, type of the event, origin of the request, and objects accessed, modified or deleted. IDS are classified as network-based or host-based depending on where they are utilized (Mukherjee et al. 1994). There are two primary approaches that IDS use to analyze events in order to detect attacks: Signature-based detection and anomaly detection (McHugh et al. 2000). Signature-based detection looks for events that match a predefined pattern of events, called as signatures, associated with a known attack. Anomaly detection techniques use a "normal activity profile" for a system and flag all system states varying from the established profile in a statistically significant manner. IDS are typically deployed within a system protected by firewalls and other access control mechanisms at the periphery. Firewalls attempt to prevent intrusions from external hackers. IDS attempt to detect intrusions from internal users as well as external hackers who have successfully cracked the firewalls. An IDS runs continually in the background, and only notifies when it detects something it considers suspicious, anomalous, or illegal. Following a signal from the IDS, a security analyst examines audit trails and log files of system resources to determine the type and the extent of the attack. If an intrusion is confirmed by the manual investigation, appropriate corrective measures are undertaken to limit further damage and recover, if possible, the damage already incurred.

Like other security mechanisms, IDS are not perfect. The likelihood of giving a warning signal upon an intrusion and being silent in case of no intrusion depends on various factors. The design of IDS, that includes the technology used (signature-based versus anomaly-based), and design parameters (for example, the acceptable noise level in an anomaly-based system) and the configuration (strict versus loose) plays a significant role. The quality of an IDS can be measured using its *false positive* and *false negative* rates. A false positive occurs when the system classifies an action as a possible intrusion when it is a legitimate action. A false negative occurs when an actual intrusion has occurred but the system doesn't classify it as an intrusion.

Model Description

Our goal is to analyze the value of IDS for IT security using a simple model that captures the essence of a typical IT security environment discussed in the previous section. To that goal we make certain simplifying assumptions. In most IT environments there are two general categories of assets relevant to the assessments of security risk: *tangible ass*ets and *intangible assets*. Tangible assets include hardware. Intangible assets, which might be better characterized as information assets, are comprised of data and software. Our model is most relevant for risks associated with intangible assets such as illegal access of information.

We assume that when an intrusion occurs, the amount of damage is distributed with probability density $f(.)$ with mean d and a finite variance known to both the firm and the intruder with support on $(0,d_{\max})$. Most companies estimate these possible damages along with their likelihoods in the IT security risk assessment phase (Tudor 2001). A fraction λ of the user traffic (both internal and external) that reaches the IDS is assumed to be dishonest.[1] It is assumed that external intruders login to the system as authorized users, and hence, the IDS cannot distinguish between external intruders and dishonest internal users. Previous studies have shown that incentives for intruders are usually not related to a financial gain.[2] Hackers tend to be motivated by curiosity, self-esteem, vandalism, peer approval, public attention, technical prowess, and politics (Shaw et al. 1999; Koerner 1999; Rothke 2000). Thus, we assume that when the hacker breaks into the system he gets a fixed utility of i. The dominant strategy of the honest users is not to misuse the system.

If an intrusion is discovered, the hacker incurs a penalty. The penalty is composed of two components: A fixed penalty β and a variable penalty proportional to the expected amount of damage, γd. The fixed penalty can be *considered* as the cost of legal prosecution and social humiliation. The variable penalty term reflects the fact that the legal system awards punishments to fit the crime (Nicholson et al. 2000). Hence, a larger damage results in a larger penalty.

Most organizations detect intrusion through some form of monitoring and analysis of audit trails (ch18 pg 223 NIST 800-12). Manual monitoring takes the form of a security team thoroughly investigating or randomly checking system log files and audit trials for possible intrusions. In general, manual monitoring is too costly to be done all the time and is done intermittently. The firm incurs a cost of c each time it performs a manual monitoring of the audit trail of a user for a possible intrusion. Manual monitoring done by the firm does not detect intrusion with certainty. This imperfection of monitoring is captured by an effectiveness parameter α, the probability with which monitoring detects a true intrusion.[3] If manual monitoring detects the intrusion, the firm recovers a fraction of the damage by the intruder without any additional cost. This fraction is captured by the parameter, ϕ.

Since manual monitoring is quite labor intensive and too costly to be done all the time, companies supplement manual monitoring with the IDS to reduce the cost of monitoring and increase the effectiveness of intrusion detection. As discussed before (IDS section), IDS use the audit trails and send a warning signal for further investigation by security investigation team. Since IDS are not perfect and produce both false positive and false negative errors, we model the effectiveness of IDS through two parameters q_1 and q_2. The parameter q_1 denotes the probability that the IDS gives a warning signal whenever an intrusion occurs. We assume that the IDS performs better than random guessing, and so q_1 lies between 0.5 and 1. That is, $(1 - q_1)$ represents the probability of false negative. Sometimes the system classifies an action as 1 a legitimate action (false positive). The complement of q_2, $(1 - q_2)$, reflects the probability of a false positive signal. Thus q_2 represents the probability that there is no signal when there is no intrusion. It is also assumed to be between 0.5 and 1 for the same reason as q_1.

We consider two different scenarios based on whether the firm has employed the IDS or not. In Scenario 1 (baseline scenario), the firm does not have the IDS in its security architecture. The firm solely relies on manual monitoring of system log files and audit trials to detect intrusive activity. In Scenario 2 the firm uses the IDS in the security architecture to complement the manual monitoring.

---

[1] We assume λ to be exogenous in our model. Theoretically, λ can be controlled by appropriately configuring the firewalls to limit entry by outsiders, and by hiring ethical employees to limit the proportion of insider hackers.

[22] Although there are some minor differences between the terms 'hacker', 'cracker' and 'intruder', these terms will be used interchangeably in this paper to describe people who intentionally compromise computer systems.

[3] We assume that the use of IDS does not alter either the cost or the effectiveness of manual monitoring because current IDS do not provide comprehensive information about the intrusion to change the parameters (pg. 124 Bace 2000). In Section 6, we discuss the implications of a potential reduction in c and/or an increase in α that may be realized if the technology underlying IDS improves in the future.

Model Analysis

No IDS Case (Baseline Scenario)

In this section we analyze the baseline scenario in which IDS is not used in the security architecture of the firm. This will allow us to establish a benchmark result that can be compared with a scenario in which the firm uses an IDS. We depict the baseline scenario in figure 1.

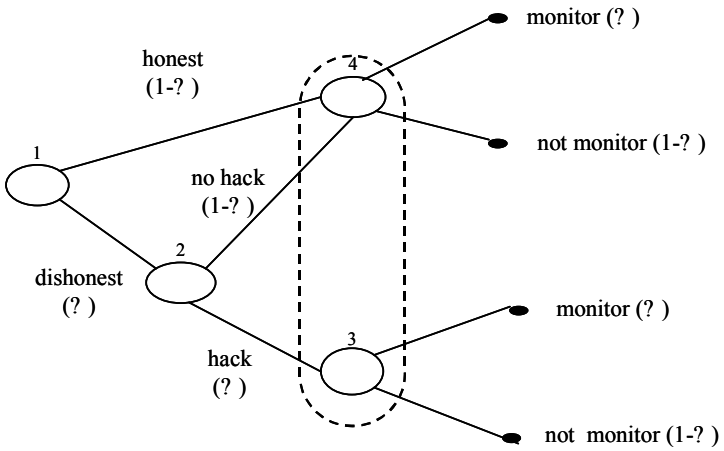

Figure 1. The Game Tree for Intrusion Detection Game without the IDS

In the game above the action set of the dishonest user is specified by $S^{th} \in \{no\ intrusion,\ intrusion\}$, where intrusion denotes to break into a system to cause an expected damage d. The pure strategy of the dishonest user is to select *intrusion* or *no intrusion* with probability one. The mixed strategy space for the dishonest user is a probability distribution ψ $\{intrusion,\ no\ intrusion\} \rightarrow$ [0,1] where ψ denotes the probability of intrusion. Similarly the mixed strategy space for the firm can be defined likewise. We denote the probability of monitoring in any mixed strategy by ρ. When implementing pure strategies, the firm either always inspects log files or ignores them completely. In mixed strategies, the firm chooses to inspect randomly with probability p.

Analysis and Results of Case 1

The objective of the hacker is to maximize his expected payoff while the firm tries to minimize the total organizational losses due to hacking. The payoff function for the firm is

$$F(\rho,\psi) = -\rho c - \lambda\psi(1-\rho)d - \lambda\psi\rho(1-\alpha)d + \lambda\psi\rho\alpha(1-\phi)d \quad (1)$$

The first term in (1) is the expected monitoring cost. The second term is the cost of not inspecting intrusions. The third term corresponds to the cost of ineffective monitoring (monitoring that is not able to catch hacking). The fourth term denotes the expected un-recovered loss from detected intrusions. A hacker's expected payoff is

$$H(\rho,\psi) = \psi\mu - \psi\rho\alpha(\beta + \gamma d) \quad (2)$$

The first term in (2) is the expected utility of the hacker from intrusions. The second term is the expected cost to the hacker if intrusions are detected. Next we summarize the equilibrium strategies for the firm and the intruder in the following proposition.

Proposition 1: The following Nash Equilibria obtains in Case1.

Equilibria	$\frac{c}{d\alpha\phi} < \lambda$	$\frac{c}{d\alpha\phi} > \lambda$
$\frac{\mu}{\alpha(\beta+\gamma d)} > 1$	$\rho = 1,\ \psi = 1$	$\rho = 1,\ \psi = 0$
$\frac{\mu}{\alpha(\beta+\gamma d)} < 1$	$\rho = \frac{\mu}{\alpha(\beta+\gamma d)},\ \psi = \frac{c}{d\alpha\phi\lambda}$	

IDS Case

This case differs from the preceding case in that an IDS is now a part of the security architecture. The game tree for this case is depicted in figure 2. The difference between the game trees of cases 1 and 2 is that in case 2 there is an additional level before the firm's decision to investigate manually where the IDS provides a signal about possible intrusive activities.

Analysis and Results of Case 2

We define $0 \le \rho_1 \le 1$ as the probability of monitoring given a signal and $0 \le \rho_2 \le 1$ as the probability of monitoring given no signal. Thus, $(1-\rho_1)$ denotes the probability of not monitoring given a signal, and $(1-\rho_2)$ the probability of not monitoring given there is no signal. When $\rho_i = \{0,1\}$ implies pure strategies, and $0 < \rho_i < 1$ implies mixed strategies for $i = 1, 2$.

When the firm observes a signal or no signal from the IDS, it updates its belief using Bayes' rule. If the firm gets a signal from IDS, it determines the posterior probability of intrusion

$$\eta_1 = \text{P(intrusion|signal)} = \frac{q_1\psi\lambda}{q_1\psi\lambda + (1-q_2)(1-\psi\lambda)} \tag{3}$$

Similarly, when the firm does not get any signal from the IDS, it calculates the probability as

$$\eta_2 = \text{P(intrusion| no-signal)} = \frac{(1-q_1)\psi\lambda}{(1-q_1)\psi\lambda + q_2(1-\psi\lambda)} \tag{4}$$

The payoff function for the firm depends on the state it is in. The payoff functions for the signal and the no signal states respectively are as follows.

$$F_S(\rho_1,\psi) = \left[-\rho_1 c - \eta_1(1-\rho_1)d - \eta_1\rho_1((1-\alpha)d + \alpha(1-\phi)d)\right] \tag{5}$$

$$F_N(\rho_2,\psi) = \left[-\rho_2 c - \eta_2(1-\rho_2)d - \eta_2\rho_2((1-\alpha)d + \alpha(1-\phi)d)\right] \tag{6}$$

The probabilities of the firm being in the signal and no signal state are $(1-q_2+\psi\lambda(q_1+q_2-1))$ and $(q_2-\psi\lambda(q_1+q_2-1))$ respectively. Thus, the firm's expected payoff at node 1 is given by

$$F(\rho_1,\rho_2,\psi) = (1-q_2+\psi\lambda(q_1+q_2-1))F_S(\rho_1,\psi) + (q_2-\psi\lambda(q_1+q_2-1))F_N(\rho_2,\psi) \tag{7}$$

The intruder's expected payoff is

$$H(\rho_1,\rho_2,\psi) = \psi\mu - \psi\alpha(\beta+\gamma d)(\rho_1 q_1 + \rho_2(1-q_1)) \tag{8}$$

Now we present the equilibria for the IDS case.

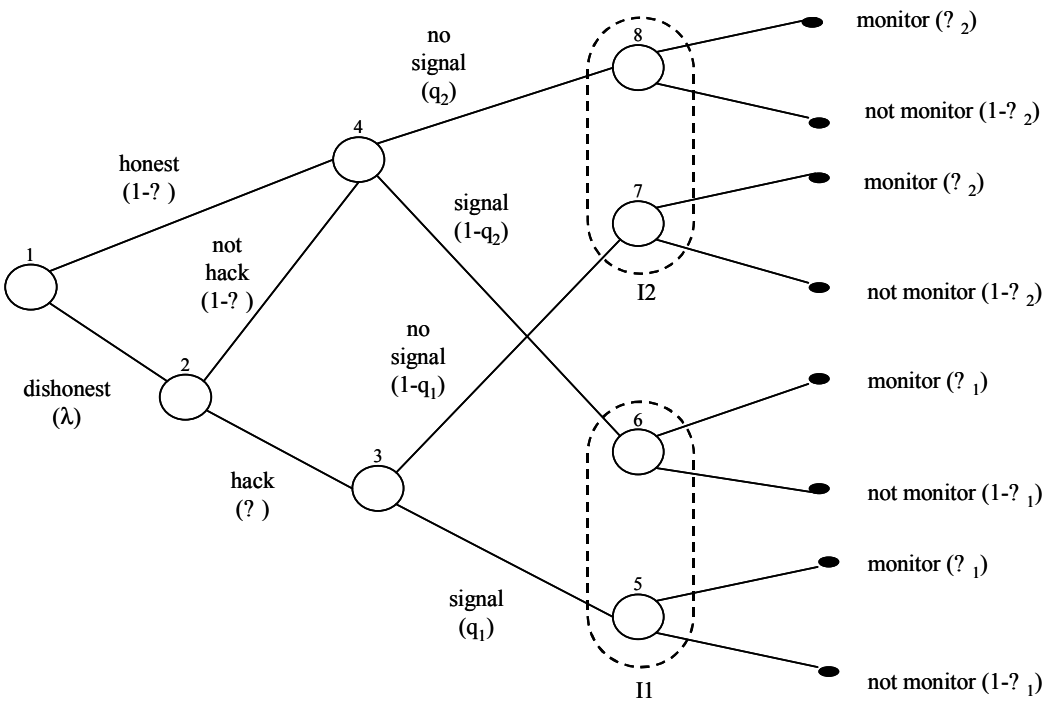

Figure 2. The Game Tree for Intrusion Detection Game with IDS

Proposition 2. The following Nash equilibria obtains in case 2

Equilibria	$\frac{c}{d\alpha\phi} < a_1$	$a_1 < \frac{c}{d\alpha\phi} < a_2$	$\frac{c}{d\alpha\phi} > a_2$
$\frac{\mu}{\alpha(\beta+\gamma d)} > 1$	$\psi=1,\ \rho_1=1,\ \rho_2=1$	$\psi=1$ $\rho_1=1,\ \rho_2=0$	$\psi=1,\ \rho_1=0,\ \rho_2=0$
$q_1 < \frac{\mu}{\alpha(\beta+\gamma d)} < 1$	$\psi = \frac{cq_2}{c(q_1+q_2-1)\lambda + (1-q_1)d\alpha\phi\lambda}$ $\rho_2 = \frac{\mu - q_1\alpha(\beta+\gamma d)}{(1-q_1)\alpha(\beta+\gamma d)}$		
$\frac{\mu}{\alpha(\beta+\gamma d)} < q_1$	$\psi = \frac{c(1-q_2)}{q_1 d\alpha\phi\lambda - c(q_1+q_2-1)\lambda}$ $\rho_1 = \frac{\mu}{q_1\alpha(\beta+\gamma d)},\ \rho_2 = 0$		

where, $a_1 = \frac{(1-q_1)\lambda}{(1-q_1)\lambda + q_2(1-\lambda)}$ and $a_2 = \frac{q_1\lambda}{q_1\lambda + (1-q_2)(1-\lambda)}$

Value of the IDS

Figure 3 illustrates the value of IDS graphically. It highlights some interesting results. In most of the parameter space, IDS either decreases or doesn't affect the firm's loss. The positive value of IDS in several regions is intuitive. The regions where there is no change to firm's loss when IDS is deployed corresponds to the extreme high monitoring cost and high hacker utility cases in which the firm's and hacker's strategies are unaffected by the presence of IDS. In region 2 and some part of region 3 IDS has a detrimental effect on total organizational loss, that is, the use of the IDS increases total loss.

As q_1 and q_2 approach one, meaning that as the firm employs a more effective IDS, regions 2 and 3 shrink, and region 1 fills up that space. In regions 1, 5, 6, and 7, the use of the IDS certainly reduces the total organizational loss. In regions 4 and 8, since equilibrium strategies for the firm and the intruder are the same under both cases, the total organizational loss is the same too, as expected. Hence there is no additional value from signal from the IDS. However as q_1 approaches one, a_1 goes to zero, and region 5 expands to cover region 4 while region 4 disappears. Similarly a_2 approaches one as q_2 approaches one. Hence, as the quality of IDS improves, the value associated with the IDS becomes positive for more firms as long as the cost of monitoring is lower than expected benefit from it (i.e. $c < d\alpha\phi$). In all other cases the firm will never monitor, hence the value of employing the IDS as a security tool will be zero.

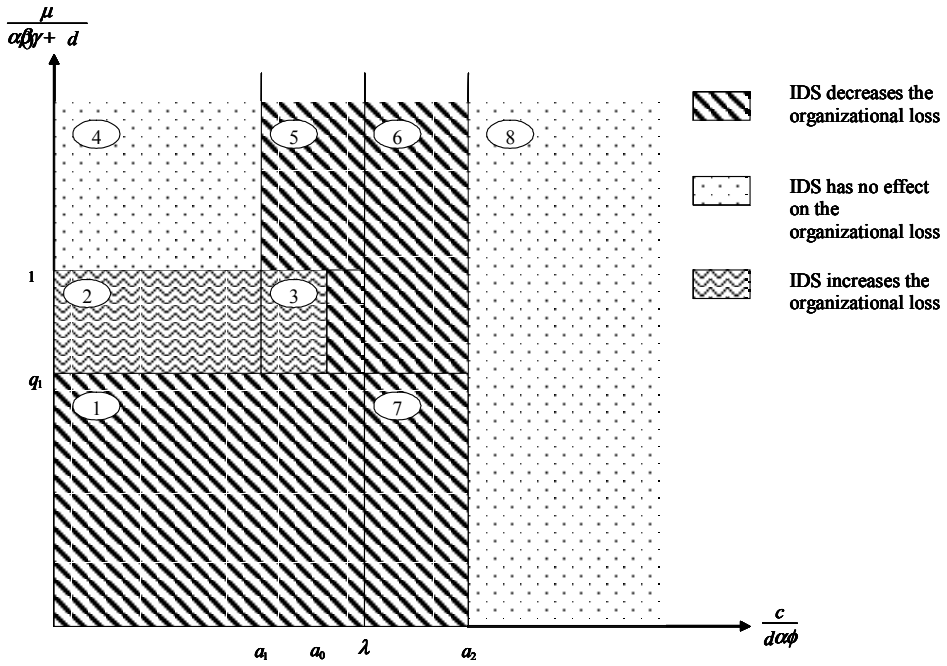

Figure 3. The Value of IDS for Different Equilibria Regions

Managerial Implications

In this section, we discuss the implications of our results for firms that seek to employ the IDS and those that develop IDS. We focus only on regions 1, 2, and 7 in discussing the implications. Our choice of these regions is motivated by the fact that only in these regions the more interesting mixed strategy equilibria occur with the IDS. In other regions, either all users hack or no user hacks. We assume that these scenarios are uninteresting.

Implication for IDS Deployers

A significant implication of our results is that not all firms benefit by deploying IDS. The location of the firm in the parameter space determines whether it benefits from IDS and the extent of benefit. The location of a firm in the parameter space depends critically on the expected damage d, among other factors. A firm with a higher value of d is riskier in some sense because it has more to lose from an intrusion. If d for a firm increases, assuming all other parameters remain the same, the firm ultimately moves into region 1, in which the firm realizes a positive value from the IDS. Thus, high-risk firms are more likely to benefit by employing IDS. We can also show that the value of the IDS is increasing in d in regions 1 and 7 implying that higher-risk firms benefit more from IDS than lower-risk firms. However, if the hacker and firm profiles are such that the firm is located in region 2, employing IDS hurts the firm. Firms that have a higher d are hurt more when using IDS within this region.

The value of the IDS is increasing in q_1 and q_2 in regions 1 and 7. Thus, a reduction in the rates of false positives and/or false negatives (i.e., a higher quality IDS) helps the firms that find IDS to be beneficial. An increase in q_1 and q_2 has the opposite effect in region 2 similar to the effect of d discussed in the previous paragraph but reduces the region itself. These results are consistent with our intuition.

We find that the proportion of hackers in the user population λ doesn't affect the value of IDS within regions 1 and 2. However, note that an increase in λ expands the total size of regions 1 and 7, indicating an increase in the likelihood of a firm being located in these regions (and, hence realizing positive value from the IDS). The value of IDS is increasing in λ in region 7. This result also implies that if a firm located in region 7 can reduce λ by employing a tighter firewall and by hiring honest employees, then the firm will find the IDS less valuable. This result is also intuitive. Preventive control mechanisms decrease the need for detective controls such as the IDS. Thus, the firewall can substitute the IDS to some extent in region 7. 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.

Probability of detection either increases or remains the same if the IDS has a positive effect on the firm. In region 7, use of the IDS increases the detection probability whereas it does not change the detection probability in region 1, meaning that the IDS not only reduces total organizational loss but also improves detection of intrusions in these regions. However, in region 2, in which the value of the IDS is negative, when the IDS is employed, the probability of detection increases only if effectiveness of manual monitoring is higher than probability of signal when there is an intrusion, and decreases otherwise.

Implications for IDS Developers

A significant insight from our analysis for the IDS developers relates to the pricing 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 firms with higher d, IDS developers may realize substantial benefits by targeting higher-risk firms. Also, industries that attract a high proportion of hackers (i.e., high λ), such as defense and financial institutions, are likely to have more firms located in regions 1 and 7. The 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.

We noted earlier that the value of the IDS to firms that benefit from the IDS increases with q_1 and q_2. Thus, an IDS developer can potentially charge a higher price for a higher quality product. A higher quality IDS will also result in a larger market for the IDS because we find that as q_1 and/or q_2 increases, the size of regions in which the IDS has positive value increases. So, more firms would implement the IDS in their security architecture. A higher quality IDS increases the price as well as demand, and hence the revenue for IDS developers. Thus, our result suggests that the IDS developers should improve the quality of the IDS in both these dimensions. However, it should be noted that the technology employed by the IDS, that is, whether the detection algorithm is based on signature analysis or anomaly detection, affects the q_1 and q_2 values. Depending on the technology used, it may be difficult to improve both q_1 and q_2 simultaneously. An increase in q_1 may decrease q_2 and vice versa. Research on IDS algorithms suggests that there may indeed be a negative correlation between q_1 and q_2 (Axelsson 2000). An interesting issue that needs to be investigated is the design of the optimal IDS based on the value of the IDS derived in this paper and costs of improving q_1 and q_2.

Although both q_1 and q_2 have positive effects on the value of IDS to firms, it is important to note that the extents of their effects are not equal. We 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.

Many of the commercial IDS are passive in the sense that their primary goal is to provide signals about possible intrusions. Only manual monitoring confirms whether there is an intrusion. The IDS also do not provide comprehensive information that reduces the effort needed in manual monitoring for confirming or rejecting the intrusion. If IDS play a more active role and thus reduce the cost of subsequent monitoring c or increase the effectiveness of manual monitoring α, we can show that the value of IDS increases substantially. A decrease in c not only increases the value but also the market size for IDS. Thus, it is worthwhile for the IDS developers to embed intelligence into the IDS in order to provide more support in the subsequent manual monitoring process.

Conclusion

IT security has become a critical issue for many firms. IDS play a significant role within a firm's security architecture. This paper investigated the value of IDS to firms. We derived the value of IDS by analyzing two cases. In the first case, we focused on a firm that doesn't employ IDS. Manual monitoring of the system log files and audit trials is the only way to detect intrusions in this case. In the second case, we analyzed a firm that uses IDS. The IDS complement manual monitoring by giving signals about possible intrusions. We derived the value of the IDS by determining the savings realized by the firm when it employs the IDS compared to the case when no IDS is used. We determined the conditions when the use of the IDS is beneficial to firms and when it is not. We also provided several implications of our results to the firms and to the IDS developers.

We made certain simplifying assumptions to model the role of IDS in an organization's IT architecture. Since formal modeling relies on abstraction to address some issues in a stylized setting, limitations are inherent to the modeling process. However analysis of an abstract model can help us understand, explain, and predict issues in realistic settings. Future research may try to model a richer IT security architecture including simultaneous design of multiple levels of preventive and detective controls. Other research avenues exist in adapting this model to different contexts, such as investment in IDS technology to improve the effectiveness of IDS. Notwithstanding these potentially attractive avenues for further research, the present study provides useful insights into how valuable IDS is in a firm's IT security architecture and implications for better IDS design and configuration.

References

Axelsson, S. "The Base-Rate Falllacy and the Difficulty of Intrusion Detection," *ACM Transactions on Information and System Security*, 3, 3, August 2000.

Bace, R. G. Intrusion Detection, Macmillan Technical Publishing, 2000.

Koerner, B. I., "Who are hackers, anyway?," *U.S News & World Report*, 17, 2, 53, July 14, 1999.

Lodin S. "Intrusion Detection Product Evaluation Criteria," *Computer Security Journal*, 15, 1-10, 1999.

McHugh, J., Christie A. C., and Allen J. "Defending Yourself: The Role of Intrusion Detection Systems," *IEEE Software*, September/October 2000.

Messmer, E. "Network Intruders," *Network World*, 16, 67, Oct. 4, 1999.

Mukherjee, B., Heberlein L. T., and Levitt K. N. "Network Intrusion Detection," *IEEE Network*, May/June 1994.

National Computer Security Center, "A guide to Understanding Audit in Trusted Systems," NCSC-TG-001, Version 2, June 1988.

Nicholson, L. J., Shebar T. F., and Weinberg M. R. "Computer Crimes," *The American Criminal Law Review*, Chicago, Spring 2000.

NIST Publication 800-12, An Introduction to Computer Security, NIST, 1996.

Power, R. "2002 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends*, 8, 1, 2002.

Rothke, B. "Hackers then and now: Answers to Some Perennial Questions," *Computer Security Journal*, 16, 3, 11-14, 2000.

Shaw, D. S., Post J. M., and Ruby K. G. "Inside the Minds of the Insider," *Security Management*, 34-44, Dec. 1999.

Tudor, J. K., Information Security Architecture, Auerbach Publications, 2001.

Verton, D., "Attorneys Debate Making Cybercrime Laws Tougher," *Computerworld*, 16, Nov. 20, 2000.