3-1-2007

Information Security Investment in Prevention and Detection Regimes – Towards an Aggregate Economic Model

Tridib Bandyopadhyay
tbandyop@kennesaw.edu

INFORMATION SECURITY INVESTMENT IN PREVENTION AND DETECTION REGIMES – TOWARDS AN AGGREGATE ECONOMIC MODEL

Tridib Bandyopadhyay
Kennesaw State University
tbandyop@kennesaw.edu

Abstract

Organizations invest in perimeter hardening as well as intrusion detection systems, but often under stand alone decision frameworks. This could mean suboptimal investments in general. For example, practitioners' approaches are more of 'satisficing' rather than 'optimizing' in nature. This paper provides methodological steps towards an integrated economic model that could seek jointly optimal investment behavior of a firm between its prevention and detection regimes of information system security management.

Keywords: IT security, IT security economic model, aggregate model, optimal IT security investment

Introduction

Security of information assets is a priority for most organizations today. Governmental regulations, customer expectations, and competitive forces all point towards further heightening of the need for adequate security of information systems. Technology and managerial issues combined; there is an apparent 2-step approach in the way an organization tends to address its information security issues.

First, organizations embrace an adequate security policy/program, train and educate its employees/users, incorporate access control, employ firewall and other network hardening devices, and encrypt communication and storage of data. These measures reduce the probability of compromise of the organization's information assets, *given an attack* from a malevolent entity. In this work, we designate it as the *prevention regime.*

Second, organizations also employ IDS (intrusion detection system) which analyze the behavior of a user in the information system (at the host server or network, as the case may be), and in case of anomalies in expected behavior/ risky or unwanted behavior, raise an alarm – upon which the administer (or the system itself) may eject the user (session termination/user isolation), or in certain situations, shutdown/isolate part or whole information system. We refer this as the *detection regime*.

The aggregate/combined level of success of this 2-step approach is however complicated by the interdependence of the (successes of the) measures at each step. Assuming that no preemptive measures could be taken to alter the behavior of a malevolent entity (who are immensely numerous anyway), managing the prior probability of an attack on an organization's information system is generally beyond the feasible scope of an information security program. The first practicable concern (and hence the intended control point as well) for an organization revolves around managing the *success of an attack* on its information system. This is manifested in the actions taken by the organization in the first step, which results in a *managed probability regime* (manifested in the residual IT security risk of the firm) that is commensurate with the accepted risk profile (posture) of the organization. In essence, *managed probability of success of an attack* then becomes the *prior probability of an intrusion* in the system, and defines the environment/paradigm of the intrusion detection management system that is to be in place.

However, the decision to eject a user or isolate/shut down a system depends on the *posterior probability* from the IDS, which may or may not bear a linear relationship with its *prior* (combined effect of *false positive* and false *negatives*). Moreover, with higher investment in prevention regime, the *managed prior* is lower, which makes an IDS alarm to be heeded with less concern (tantamount to an addition to the IDS's systemic false positive pool), and

an absence of an alarm to be relied with higher confidence (a theoretical addition to the IDS's systemic 'false negative' pool), both of which potentially lessen the efficacy of the IDS system. In the dual dimension, the fact that a downstream intrusion detection system is in place (a second line of defense), investment in step-1 could experience moderating effects as well. The cyclic nature of these effects allude to the need of a combined decision framework in which the investment decisions in both the steps could be coordinated for the overall optimal level of information security that an organization may strive to achieve.

The following questions are important to consider in the above scenario of integrated decision making process:

1. How should an organization allocate/apportion funds such that an optimal level of security is achieved in the prevention (managed probability) regime?
2. Given a prevention/hardening scheme is in place, what is a minimum schedule (cost vs. level of efficiency) that an IDS must offer in order to justify its inclusion in the security initiative of an organization?
3. Given a coordinated investment regime, what are the systemic factors that could modify investment in either of the approaches?
4. If a firm internalizes its decision of perimeter hardening while operationalizing an IDS scheme, how do the investments differ from the above?

Although most large organizations invest in both the above, there appears to be no extant aggregate planning approach to coordinate the *optimal* investments between these steps of information security technologies.

The most accepted approach in practice, centered on the metric *ROSI*, is an accounting approach and is predominantly *satisficing* in nature. Like ROI, ROSI implicitly requires a comparison framework - be it a framework of competing technologies or initiatives, or against an organizational *hurdle rate* of (risk adjusted) return. If the framework is comparative, ROSI is utilized to arrive at the best investment decision *given the set of competing possibilities/options*. On the other hand, the hurdle rate for IT security projects may be a (organization specific) general hurdle rate, or a benchmarked or baselined ROSI, which are again subsets of selection. In essence, accounting methods of investment decision (e.g. ROI and ROSI) tend to justify (or not) the given costs of a technology or initiative (and also among other competing possibilities), when the expected benefits are known in relation to the organization's internal and environmental business parameters. This process is tantamount to a *bounded rational* behavior and would not ensure an optimal overall level of investment in IT security initiatives.

On the other hand, academic researchers and theoreticians have focused on economically optimal levels of a firm's security investment in mainly 3 categories:

1. Where the firm's security investment is composite but independent (Heal et al., 2003),

2 Where firm's security decision is interdependent yet composite (Gordon et al., 2000), and

3 Where firm's security investment decisions are coordinated in two different regimes - those of technological and financial instruments (Gordon et al., 2003, and Ogut et al., 2004).

In contrast to the practitioners' approach, this research attempts to find a model that could derive the optimal investment level for the organization in the true economically rational sense.

As against the above streams of academic and theoretical research, this research concentrates in the firm's investment in the technology instruments (financial instruments have not been much popular in IT risk management yet), but instead of treating the technology investment in a composite manner, separates the prevention (perimeter hardening) and detection (IDS schemes) in a two step integrated process, such that available technology budget of the firm could be judiciously allocated between them.

This is an ongoing research, and this initial report explains the development of the proposed (integrated) model and its justification in the light of joint optimality of security investment decisions between the prevention (hardening) and detection regimes. The rest of the paper is organized as follows: Section-2 describes our basic assumptions, and develops the integrated model of investment decisions between prevention and detection regimes. This section also provides some initial observations on investment decisions. Section-3 develops a numerical example to illustrate the relative levels of investments. Section-4 discusses proposed future work and concludes this report.

Assumptions, Model Development, and Initial Observations

Assumptions

We assume (without any loss in generality) that there exists one unique technology each for prevention and Intrusion Detection. We also assume that decision of investment in prevention is a continuous decision (a pervasive organizational effort with higher flexibilities) whereas the decision to invest in IDS is a discreet choice (single or multiple binary choices, network or host level technical implementation)

Model development

The model is developed through the following 3 progressive cases:

Case - I

This is the body of the paper. Suppose that the prevention technology provides an efficacy that is mapped through a firm specific (TTF[1]) technology transfer function, $p(c_h)$ as depicted in *figure-1*. Thus if the firm invests c_h in its prevention regime, the post investment probability that a hacker/unauthorized user would succeed to compromise the information assets is $p(c_h)$. The above assumption is consistent with standard economic prudence of diminishing marginal return from the IT security investment. The TTF is assumed convex, and hence all convexity assumptions in IT investment apply as well: $p'(c) \leq 0,\ p''(c) \geq 0$. In absence of any investment by the firm (given an attempt), the unauthorized user is expected to be successful in compromising the firm's information asset with certainty: $p(0) = 1$. On the other extreme, the above TTF is asymptotic to the investment axis, and implements the fact that with our current level of prevention technology, no finite investment may ensure complete impenetrability: $p(\Psi) = 0, \quad iff\ \ \Psi \to \infty$.

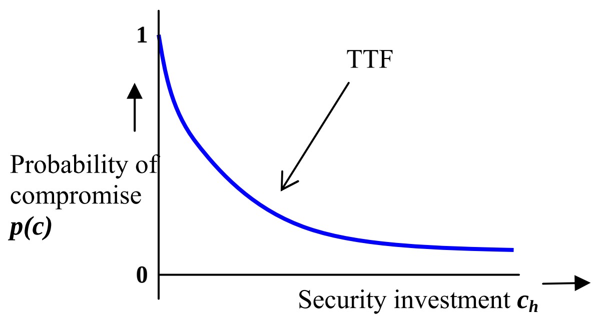

Figure1. Technology Transfer Function (TTF) of security investment

We will also assume that if an attack is successful, a total loss of L is incurred to the firm. The firm now optimizes the following expression:

$$\underset{c_h}{Max}\left(-c_h - p(c_h)L\right) \qquad \text{...} \qquad (1)$$

The optimal investment for the firm is given by the first order condition of (1), thus the firm invests: $c_h{*} = p'^{-1}\left(-\frac{1}{L}\right)$. This result is simple and intuitive: when a firm has higher loss expectancy L, its optimal level of investment in security increases monotonically.

---

[1] Some conceptual detail of the TTF has been provided while describing the numerical example.

Case - II

When the firm also invests in detection technology, it achieves a second level of protection over and above the managed probability regime of **case-1**. Assuming that the cost of an IDS regime[2] is c_i : given an unauthorized user in the firm's network, the ID system identifies the intruder with a probability q. Knowing that the IDS works on top of the managed probability regime, the firm now optimizes the following[3]:

$$\underset{c_h, i}{Max}\left(-c_{h,i} - c_i - p(c_{h,i})(0+(1-q)L\right) \qquad \text{.....} \qquad (2)$$

As before, the optimal investment in prevention is arrived from the FOC of (2): $c_{h,i}{}^* = p'^{-1}\left(-1/(1-q)L\right)$. Noticing that $1 \geq q \geq 0$, it is apparent that the optimal level of investment in perimeter hardening is now lower with IDS than without. Intuitively, in presence of a second line of defense, the optimal investment in perimeter security drops from case-1 to case-2. *Figure-2* depicts this change in the optimal investment in network hardening. The FOCs of (*1*) and (*2*) yield $p'(c_h{}^*)$ and $p'(c_{h,i}{}^*)$, which, once projected on to the (*TT*F) acceleration curve $p'(c)$ yield the optimal investments $c_h{}^*$ and $c_{h,i}{}^*$, and their corresponding optimal probabilities $p(c_h{}^*)$ and $p(c_{h,i}{}^*)$: the arrowheads are drawn in a consistent fashion to facilitate understanding of the above.

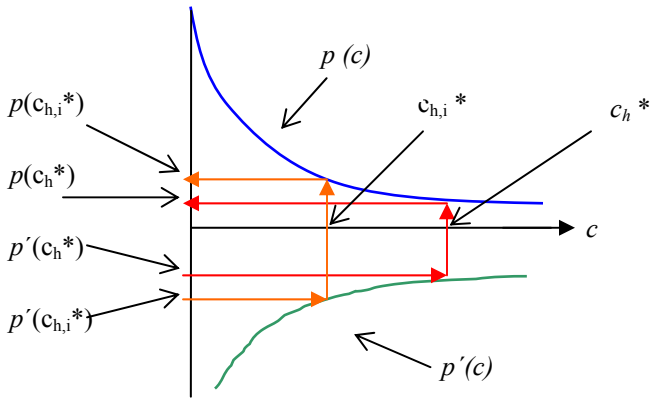

Figure2. Optimal Investment in hardening (implicit form)

Finally, the firm decides to implement an ID system over and above its prevention regime only when the cost of available IDS conforms to the following relation:

$$c_i \leq p'^{-1}\left(-1/L\right) - p'^{-1}\left(-1/(1-q)L\right) \qquad \text{.....} \qquad (3)$$

Sub-case - IIA: In case there exist competing products/technology of IDS, or there are *j* options in terms of depth and breadth of implementation of IDS, a schedule of the cost-efficiency couples (c_{ij}, q_j) of the detection schemes can be drawn, and the final selection could be optimally made from the following:

$$\underset{j}{Min}\left\{\left[c_{ij} + p'^{-1}\left(-1/(1-q_j)L\right)\right]\right\} \qquad \text{.....} \qquad (4)$$

$$subject\ to: \quad c_{ij} \leq p'^{-1}\left(-1/L\right) - p'^{-1}\left(-1/(1-q_j)L\right)$$

[2] The assumed cost is composite of procurement and operation of the IDS system in general.

[3] $c_{h,i}$ is the investment of the firm when investment in prevention necessary is associated with that in IDS.

Case - III

A Closer look at the IDS paradigm, however, warrants further refinement. An IDS generally needs added interventions in view of its innate operating problems known as 'false positives' and 'false negatives'. This calls for a moderation of our assumed (efficiency) notation ***q***, and we bring that moderation in the following fashion:

We assume that a) given an intrusion, the IDS (rightly) provides an alarm with a probability ***q***, and b) given no intrusion, the IDS (falsely) provides alarm with a probability ***r***. Because an alarm requires further investigation/action by the firm personnel, a false alarm is nonetheless costly (***l***), although the information assets of the firm are not compromised (we initially internalize this is a system loss, and not an operational cost, which we have included in our composite cost of the IDS, c_i). On the other hand, if the IDS fails to provide an alarm when an intruder is in the network, we assume that the loss of information asset is, as before, L.

Under the modified assumptions and loss/cost structures, the expected loss of the firm is now modified to $\left(p(c_{h,i})\{q.l+(1-q)L\}+(1-p)\{r.l+0\}\right)$, and the firm now solves the following:

$$\underset{c_{h,i}}{Max}\left(-c_{h,i}-c_i-p(c_{h,i})\{q.l+(1-q)L\}-(1-p)\{r.l+0\}\right)\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (5)$$

Again, the FOC of (3) yields the modified optimal investment in prevention technology of the firm: ${}^{m}c_{h,i}^{*}=p'^{-1}\left(-1\Big/\{(1-q)L+(q-r).l\}\right)$, where the superscript ***m*** highlights the currently modified structure of the problem.

Initial observations

Comparing ${}^{m}c_{h,i}^{*}$ with $c_{h,i}^{*}$, the following observations are in order now:

Observation - I

As for all practical purposes the operating characteristics of the IDS must ensure $q>r$ (else any randomizing device could replace our IDS!), ${}^{m}c_{h,i}^{*}>c_{h,i}^{*}$. Clearly, investigation related losses of false positive alarms adversely affect the efficacy of the IDS, and the firm tends to invest proportionally more in perimeter security now. Note that the treatment of investigation cost '***l***' as a system loss is important here - the firm may exercise control in tuning its IDS (***q*** and ***r***), and thus the internalization of this effect as a loss is more apt than considering it as a cost.

Observation - II

So long $L > l$, even with the problems of false positive and false negative in the IDS operations, the investment in perimeter security in the combined regime remains strictly lower than the managed probability regime: $\forall L>l$, the required precondition $\left[(q-r)\Big/q\right]\geq L\Big/l$ is absurd.

Observation - III

Using ${}^{m}c_{h,i}^{*}$ as an analog of $c_{h,i}^{*}$ in to (*3*) and (*4*) yield the decisional criteria for selection and procurement decision of an IDS in view of the innate problem of false positive and false negative of an IDS.

Numerical Example

In order to augment appreciation of the problem of joint optimization (the analysis is in implicit form,) here we present a numerical example to highlight the differences in investments under the three different cases. Suppose that

the prevention technology TTF is given by $p = e^{-kc}$ where ***k*** is a firm specific factor (a higher value of ***k*** achieves higher benefit from the same investment ***c*** for a firm, and could depend on the security readiness of the firm, and its current level of maturity in pertinent learning curves).

Thus, $p' = -kp$, and the optimal investments are listed as below:

$$c_h^* = \frac{Ln(LK)}{K}, \quad c_{hi}^* = \frac{Ln(LK(1-q))}{K}, \quad {}^m c_{hi}^* = \frac{Ln\{LK(1-q) + lK(q-r)\}}{K}.$$

Thus, if $L = \$1000, \quad K = 0.01, \quad l = \$10, \quad q = 0.8, \quad r = 0.2$, the following values of the optimal investment in perimeter technology could be compared: $c_h^* = \$230, \quad c_{hi}^* = \$69, \quad {}^m c_{hi}^* = \$72$.

Clearly, any IDS scheme which cost between $\$158$ *and* $\$161$ is no longer feasible for the firm when the idiosyncratic problems of an IDS are considered.

Limitations, Future Work, and Concluding Remarks

My goal in this research is to internalize the firm's investment decisions of prevention and detection technologies in an interdependent fashion, such that a more complete joint optimization of the hitherto disparate decisions could be examined. This work is in its very initial phase, and the current internalization of investment effect interdependency is through the losses from the false positive alarms of the IDs. This is a definite limitation of the research in its current stage, although even this simple internalization has provided some important observations. I propose to further internalize the investment interdependency by making both ***q*** and ***r*** functions of the investment decision of the firm in its prevention regime i.e. $\boldsymbol{q = q(c_{h,i})}$ and $\boldsymbol{r = r(c_{h,i})}$. This internalization will not only bring out the optimal investments in prevention and detection regimes, it will also likely calibrate the firm's most advantageous tuning of the implemented IDS. This proposed approach is however challenged by a possible complication of the mathematical analysis of the model. In such case, I envision a partial mathematical solution augmented by a thorough numerical analysis which could bring out the insights in an effective fashion.

References

Gordon Lawrence A., and Loeb Martin P. (2002) The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457.

Gordon, Lawrence A., Loeb, P. Martin and Sohail Tashfeen. (2000) A framework for using insurance for cyber risk management. Communications of the ACM, 46(3), 81-85.

Heal G., and Kenreuther H. (2003) You only die once: managing discrete interdependent risk. National Bureau of Economic Research, USA.

Ogut, H., Srinivasan, R., and Menon, N. (2004) Self protection and insurance in IT security: the case of interdependencies. Working Paper. The University of Texas at Dallas.

Rasmussen E. (1989) Games and Information – An introduction to game theory. Second Edition. Blackwell Press, USA.

Sonnereich W. (2006) Return on security investment (ROSI): a practical quantitative model. Sage Secure LLC, USA. Accessed at www.sagesecure.com.

Varian, H. (2002) System Reliability and Free Riding. Working Paper. The University of California at Los Angeles.