Justifying Spam and E-mail Virus Security Investments: A Case Study

Hemantha Herath[1] and Tejaswini Herath[2]

Abstract: Our paper investigates the problem of justifying security investments concerning spam and email virus using real life data from a midsize North American university. We formulate the spam and email virus security problem as a capital budgeting problem using operating characteristic (ROC) curves in a decision theoretic framework. Prior research has investigated the optimal configuration in a detection system focusing on hacking. In a corporate setting when making the case for information security not only the technology specific detection costs but other costs (capital expenditures, operating costs and opportunity costs) have to be considered. We contribute to the current literature by investigating the spam email and virus problem and demonstrating how theoretical research can really be applied in practice through a real life case study.

1. Introduction

Investments in information security have been recognized as an important issue by both practitioners and academics alike. However, what should be the Return on Security Investments (ROSI) and the appropriate level of investments has been a controversial topic (Cavusoglu et. al. 2004). The return on security investment or the loss without security investments is hard to quantify due to difficulty in defining and measuring the full array of benefits. The impact of information security breach may well be financial, in the form of costs (increased insurance costs, equipment rental/purchase for recovery, overtime costs, etc.), loss of productivity, revenue (direct loss of

[1] Corresponding author, Associate Professor of Managerial Accounting, Department of Accounting, Faculty of Business, Taro Hall 240, 500 Glenridge Avenue, St. Catharines, Ontario, Canada L2S 3A1.; Tel: (905) 688-5550 Ext. 3519; Fax: (905)688-9779; E-mail: hemantha.herath@brocku.ca

[2] Doctoral student, Department of MIS, State University of New York at Buffalo, NY, USA

downtime, lost future revenues), and financial performance (credit rating, stock price). However, more serious are the difficult to quantify or the hidden costs such as damaged reputation that may have a negative impact on customer, supplier, financial market, banks and business alliance relationships (Camp and Wolfram 2004).

Despite of the controversy surrounding ROSI , it is widely recognized that organizations have become so dependant on computer based and telecommunication intensive information systems that disruption of either may cause outcomes ranging from inconvenience to catastrophe. As e-commerce continues to grow, so will cyber crime and the need for IT security. Information security which once was considered as just overhead costs is now widely recognized as an important investment of business operations (Cagnemi, 2001).

Corporate spending on information security continues to grow significantly. This has resulted in a growing stream of research in information security. Gordon and Loeb (2002) however, point out that much of information security research has focused on technical aspects of information security (such as encryption, bandwidth, intrusion detection software and security architecture) or behavioral aspects of reducing information security breaches while there has been very little research devoted to the economic aspects of information security.

Along with the traditional approaches mentioned in numerous textbooks, several researchers have investigated economics of information security. The seminal research in this area can be identified with the work of Gordon and Loeb (2002, 2003) and Cavusoglu and Raghunathan (2004), Cavusoglu et.al (2005). As discussed in Cavusoglu (2004), researchers have considered different approaches to determine the effective level of IT security investments. For example, Hoo (2000) provides a traditional decision analytic framework to evaluate different IT security policies based on cost-benefit tradeoffs. He considers not only the costs of security controls and expected loss from security breaches but also additional profits expected from new opportunities. Longstaff et.al (2000) show that investment in systematic risk assessment reduces the likelihood of intrusions yielding benefits much higher than the investment cost. Gordon and Loeb (2002) propose a model to identify the optimal level of security investment (an interior optimal solution) based on the identification of potential security violations in terms of their damage and likelihood. They argue that allocation of funds to information security should be similar or at least based on cost and benefit terms similar to allocating funds to any other activities using capital budgeting techniques such as net present value (NPV) or more advanced real option techniques and/or game theory. Cavusoglu and Raghunathan (2004), Cavusoglu et.al. 2004, 2005) explore the optimal configuration of detection software by using decision and game theory approaches. Their framework is more rigorous since it allows features specific to IT technologies to be considered.

While these studies provide valuable insight into different security vulnerabilities including hacking there is no “one size fit all” type model solution. For example, the game theory approach tries to analyze the optimal security investment problem as a game between a hacker and the organization. It is unique to situations of intrusions where a hacker has a motive against a particular organization. However, in a scenario such as the security problem of spam and e-mail virus, which this paper focuses on, the malicious user may not have a motive against a particular organization. Then it may be more appropriate to treat the security problem as a game against nature. In a spam and virus email security scenario the game theoretic approach may not be the best approach but decision theoretic methods seem more appropriate.

Our paper investigates the problem of justifying IT security investments concerning spam and email virus security using real life data from a midsize North American university. We formulate the spam and email virus security the problem as a capital budgeting problem using operating characteristic (ROC) curves in a decision theoretic framework as in Ulvila and Gaffney (2004) and Cavusoglu and Raghunathan (2004). Cavusoglu and Raghunathan (2004), focus on finding the optimal configuration (i.e. optimal quality parameters) in a detection system. In a corporate setting when making the case for information security not only the technology specific detection costs but other costs (capital expenditures, operating costs and opportunity costs) have to be considered. We contribute to the current literature in two ways, first, by investigating spam and email virus security problem. Second, demonstrating how theoretical research can really be applied in practice through a real life case study.

The paper is as follows. Section 2 starts with the case example by providing a brief description of an university email service architecture currently in place and configuration alternatives. Section 3 summarizes prior work that identifies specific features of information technology security. In section 4 we incorporate these configuration specific characteristics in a capital budgeting model that can be used to make the case for investments in IT security investments. Section 5 provides an application example with real data and section 6 concludes.

2. Existing University Email Service Architecture

The north american university (hereafter referred to as NAU) considered in this study is a midsize university with over 18,000 full and part time students with approximately 1200 staff and faculty. We consider the e-mail services at this university as our application case study.

Many recent surveys report that viruses pose a significant threat to information technology systems. The 2004 eCrime watch survey reports that virus and other malicious codes were the most frequent type of electronic crimes (77%) experienced by organizations. SPAM and phishing e-mails also ranked high in the list of electronic crimes committed. A recent CSI/FBI survey (2004) notes that, although attacks on computer systems have declined steadily in last few years, virus attacks remains highest compared other types of attacks causing maximum dollar losses. While there are various sources for virus propagation, the 2004 ICSA survey shows that virus propagation by e-mail pose the greatest threat. As illustrated in Table 1 in recent years email vectors continues to be the primary means of virus spread.

Table 1: Virus Propagation

Virus Source	1996	1997	1998	1999	2000	2001	2002	2003
E-mail Attachment	9%	26%	32%	56%	87%	83%	86%	88%
Internet Downloads	10%	16%	9%	11%	1%	13%	11%	16%
Web Browsing	0%	5%	2%	3%	0%	7%	4%	4%
Don’t Know	15%	7%	5%	9%	2%	1%	1%	3%
Other Vector	0%	5%	1%	1%	1%	2%	3%	11%
Software Distribution	0%	3%	3%	0%	1%	2%	0%	0%
Diskette	71%	84%	64%	27%	7%	1%	0%	0%

Source: ICSA Labs 9th Annual Computer Virus Prevalence Survey, 2004

In addition to the direct damage the virus e-mails pose, spam e-mails also adversely affect organizations. Spam e-mails affect the productivity of the employees, e-mail server storage space and have bandwidth implications. Organizations continue to deal with these problems using several mechanisms. For example, organizations may use different e-mail server architectures depending resource availability and security levels. Figure 1 depicts the architecture used for e-mail services at NAU.

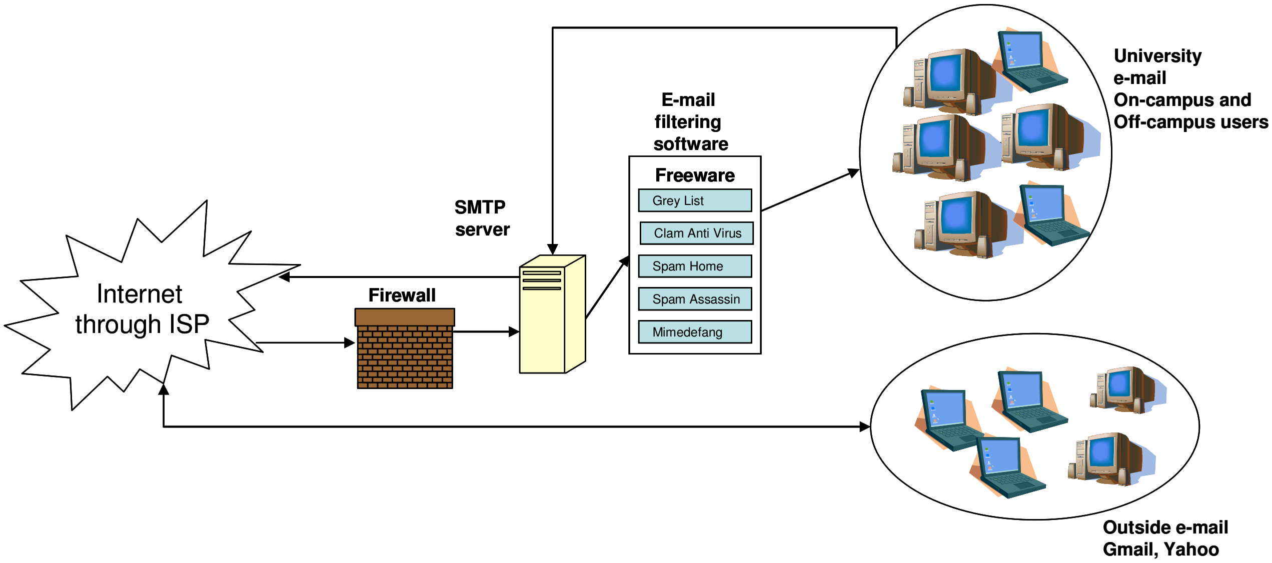

Figure 1: E-mail services architecture

All incoming e-mails with NAU e-mail address passes through a firewall. Along with other activities, the firewall checks the e-mail (as well as web) traffic for any potential virus infections. The allowed-to-pass (ATP) through e-mail traffic is then diverted to SMTP server. The emails are stored on the SMTP server till they are retrieved by the e-mail recipient. Several filters are configured to identify malicious or spam e-mail. Since all organizational e-mails are filtered, the location of a recipient whether on-site (at university premises) or off-site does not make difference. However, e-mails received on third party e-mail services such as Yahoo, GMail, Hotmail and others, do not get scanned and therefore increase NAU's systems vulnerability. In Table 2 we tabulate e-mail transactions data for a two day period from NAU system for its existing configuration which we call Option II. As seen there are 238 detected virus infections in a span of two days. These along with other non-productive e-mails such as SPAM and phishing, pose a significant productivity as well as IT security issue to NAU.

Table 2: NAU E-mail Statistics (October 24-26, 2005)

Outgoing	200866
Incoming	671512
Total e-mail transactions	**872378**
Incoming	
Virus	298
Spam	9924
Reject	180575
Longform User	32566
Grey	133672
Triplet (White, Black, New) and Misc	162001
Passed	34877
Accepted	37655
Mail in	79944

2.1 Architecture for e-mail Security

In Figure 2 we show the e-mail filtering process at NAU. All external traffic including e-mail and web traffic passes through the firewall. The unauthorized traffic filtered by the firewall is dropped and remainder is passed to appropriate servers. E-mail traffic which is routed to SMTP server can originate from both known and unknown sources. E-mails from unknown sources are subject to extra scrutiny. E-mails considered malicious are dropped and others grey listed for further investigation. One type of investigation to verify authenticity includes requesting the sending machine to resend the e-mail message within a specified time (say 20 minutes). If the resent email is again received by the NAU server within the stipulated time then the sender is assumed to be authentic. That message is removed from grey list and delivered to the intended recipient. However, if the sender is not authentic and the messages are not resent as majority times in case of spam, then the messages are dropped. Other filters have different processes for verifying authenticity. Based on the configuration that allows the extent of monitoring, a signal score is calculated and compared against a threshold to classify an email as harmful or harmless.

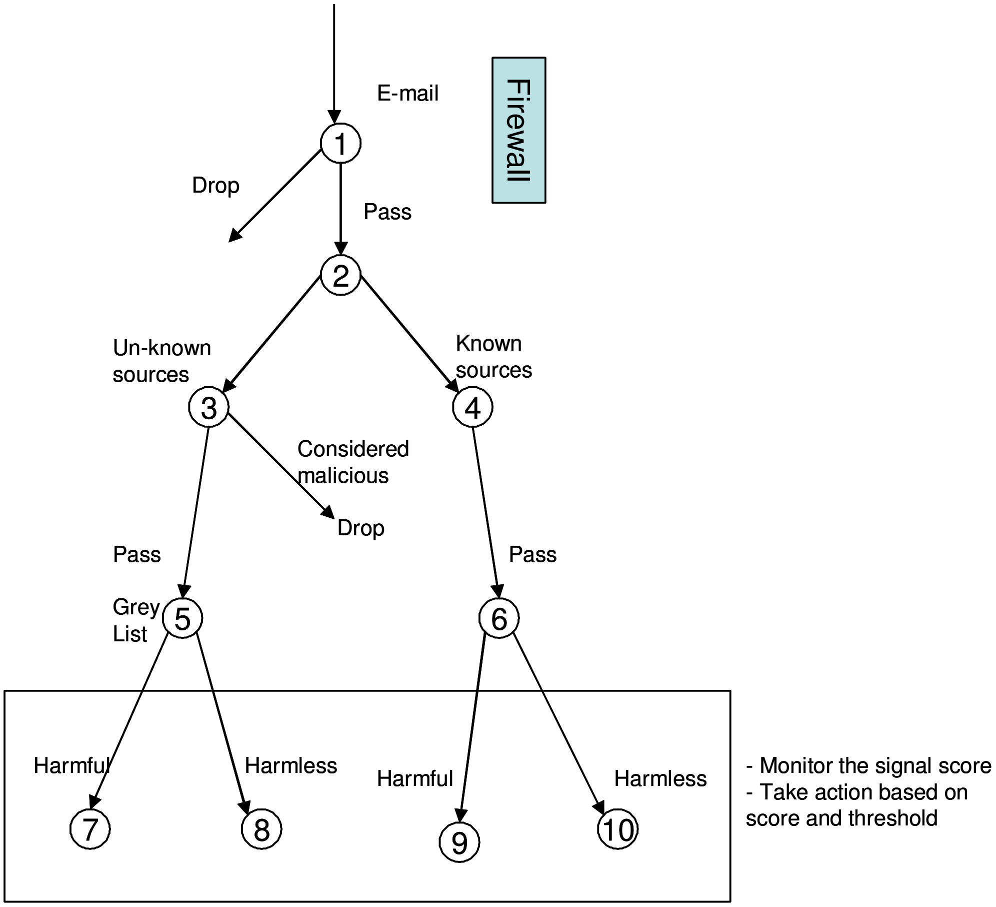

Figure 2: NAU Email Filtering Process

2.3 Security Configuration Alternatives

There are many filters available as freeware, which are quite effective. However, these filters need to be configured and that requires skilled labor. Depending on the level of the security desired the labor hours allocated to configurations may vary. Off-the-shelf products are also available which need relatively less number of, nearly negligible, hours to implement. However, the cost of the product as well as the level of security it provides may differ from an in-house developed configuration.

At the time of investing in IT security at NAU, several options were available to the decision makers as shown in Figure 3. These include option I (low level of security configuration), option II (medium level of security configuration), option III (high level of security configuration) and option IV (off-the shelf box). The decision makers also had to argue the case for which configuration would be the best given NAU's budget, as many other universities NAU operates on a tight annual budget. Figure 3 shows capital expenditure costs in the implementation phase. Next sections details how IT investment planers could make the case for justifying IT security spending.

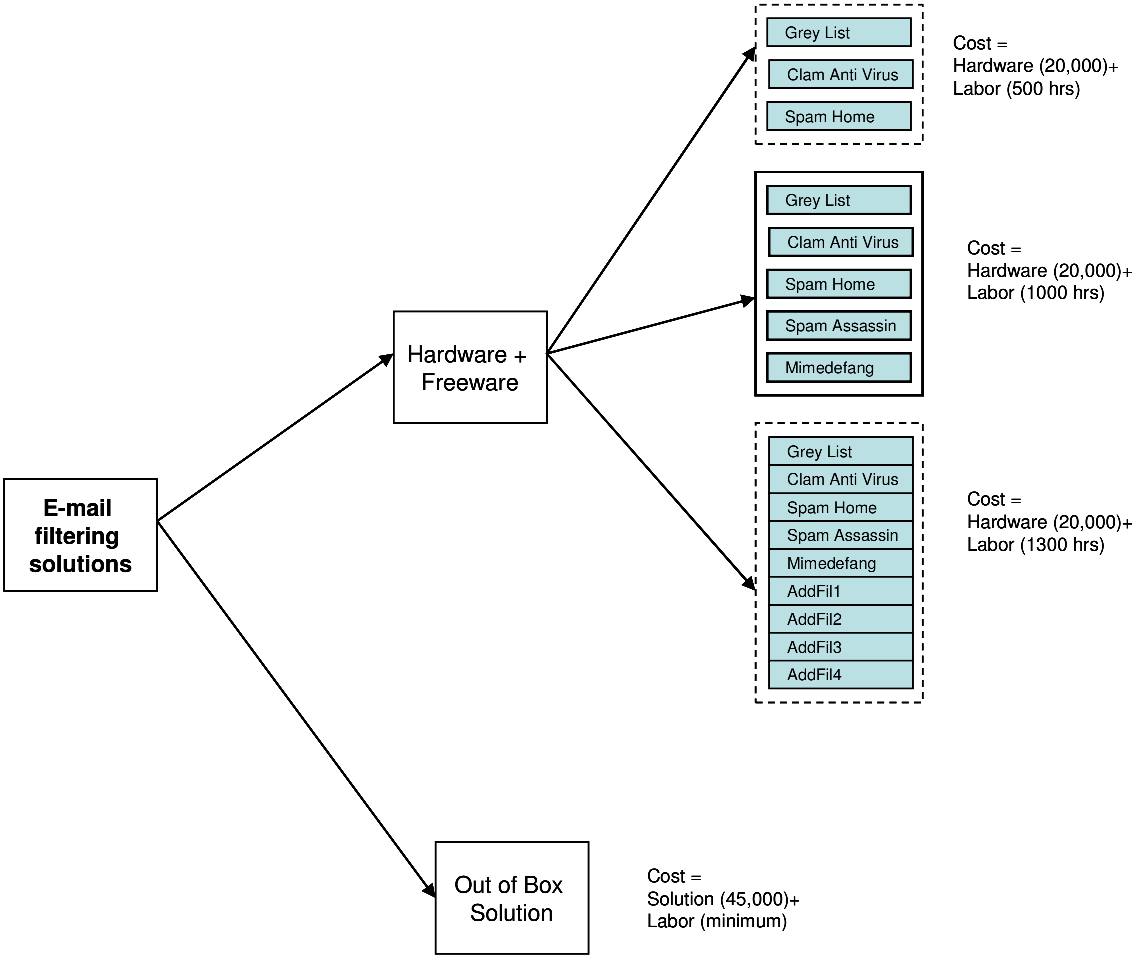

Figure 3: Configuration Alternatives

3. Prior Related Research

We follow the receiving operating characteristic (ROC) approach by Ulvila and Gaffney (2004) Cavusoglu and Raghunathan (2004) for comparing the effectiveness (or quality profile) of different configuration of the email gateways. The approach is based on classical statistical theory where the ROC curve provides the relationship between the two classification errors in a detection system. The two error classifications are false positive which occurs when the system classifies an authorized transaction as malicious and false negative where a malicious transaction is classified as authorized.

We use similar notation used by above authors to be consistent[3]. Let s be a numerical score used by detection software based on transaction data and t the threshold score. The system classifies a transaction as a malicious/fraudulent if $s > t$. The numerical scores for authorized (normal) transactions s_N and unauthorized (fraudulent) transaction s_F is assumed to follow exponential distributions with parameters λ_N and λ_F. Define $r = \frac{\lambda_F}{\lambda_N}$ as the ratio of mean score of normal transactions to that of fraudulent transactions. Then the relationship between the quality parameters of the detection system, probability of detection P_D and probability of false positive P_F is given by the ROC curve as $P_D = P_F^r$. Notice that if one denotes an authorized transaction as H_0 and an unauthorized transaction as H_1 then, $P_D = \Pr(H_1 | H_1 \text{is true})$ and $P_F = \Pr(H_1 | H_0 \text{is true})$. There is also the error of a false negative given by $1 - P_D = \Pr(H_0 | H_1 \text{is true})$ but, this is taken care of by P_D itself.

The decision tree for configuring a detection system is shown in Figure 4. The detection uses the scored transactions to provide signal to flag the state of the transaction as an unauthorized transaction a “signal (i.e. with probability x) ” or not classified as unauthorized a “no signal

[3] To avoid confusion, for the numerical score, we use s here instead of x as x is also used for the probability of a signal.

(i.e. with probability $1-x$)". Let ψ denote the proportion of malicious emails, then the probability of a signal and no-signal are given by:

$$\text{P(signal)} = x = P_D\psi + P_F(1-\psi) \qquad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

$$\text{P(no - signal)} = 1 - x = (1-P_D)\psi + (1-P_F)(1-\psi) \qquad \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Using the Baye's rule then one can obtain the following posterior probabilities

$$\text{P(malicious} \mid \text{signal)} = \eta_1 = \frac{P_D\psi}{P_D\psi + P_F(1-\psi)} \qquad \ldots\ldots\ldots\ldots\ldots\ldots(3)$$

$$\text{P(malicious} \mid \text{no - signal)} = \eta_2 = \frac{(1-P_D)\psi}{(1-P_D)\psi + (1-P_F)(1-\psi)} \qquad \ldots\ldots\ldots\ldots\ldots\ldots(4)$$

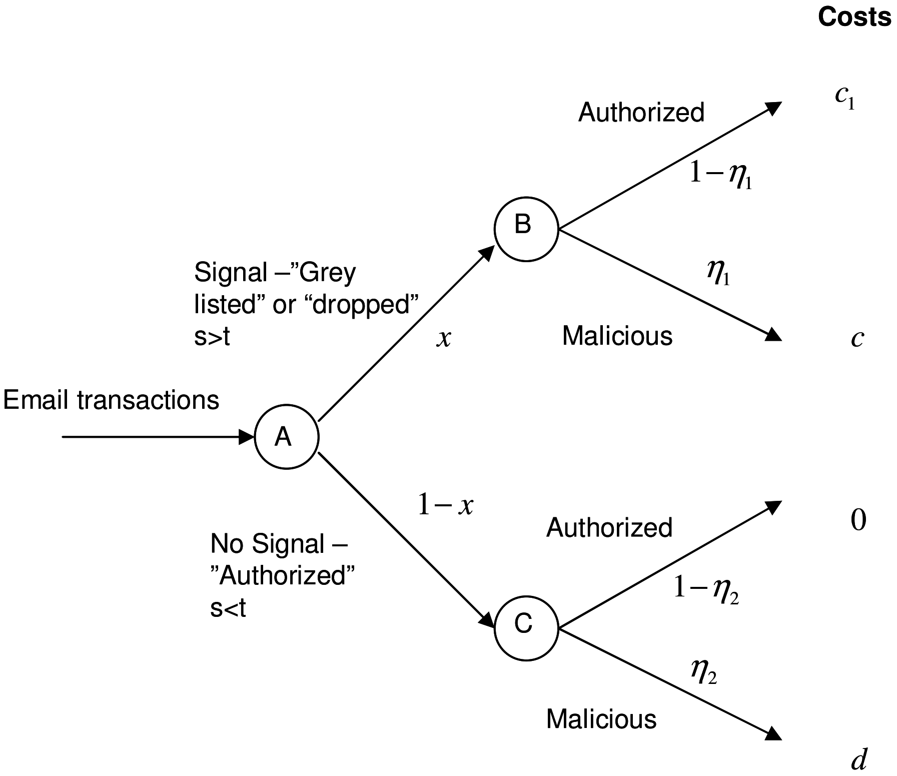

Figure 4: Probability tree for a given Configuration

We assume that if the detector signals a fraud then it is investigated and if it does not signal it is not investigated. This is a simplifying assumption but can be relaxed as in Cavusoglu and Raghunathan (2004) where a decision will be taken in both signal and no-signal state whether or not to investigate. The costs pertaining to the terminal states are shown in Figure 4. We define (c) as the cost of an investigation for correctly signaled malicious e-mails, (c_1) as opportunity cost of lost productivity plus the cost to investigate if an authorized transaction is incorrectly signaled as malicious, and (d) as the damage from an undetected fraud. Using equations 1, 2, 3 and 4 and taking the expected values at each node in the probability tree and folding back we compute the expected cost of the detection system configuration as a function of the quality parameters P_D and P_F of the system given by

$$E(C_D) = cP_D\psi + d(1-P_D)\psi + c_1P_F(1-\psi) \qquad \text{………………………}(5)$$

This result is identical to the firm’s expected cost under Region 2 in Cavusoglu and Raghunathan (2004), pg 137. Our simplification, whether or not to investigate did not impact the cost since Regions (1) and (3) are of no interest to system evaluators as proved in Cavusoglu and Raghunathan (2004).

In Cavusoglu and Raghunathan (2004), under the decision theory approach, the optimal configuration (i.e. optimal quality parameters) is found by minimizing Equation 5. While this approach provides the corner solution of the configuration it does not consider how the information systems budget would affect the system configuration or the capital budgeting problem. In the next section, we incorporate configuration specific characteristics in a capital budgeting model that can be used to make the case for investments in IT security investments.

4. Investment Model

Every security system has costs and requires tradeoffs. Most security costs money, sometimes substantial amounts; but other tradeoffs may be more important, ranging from matter of inconvenience and comfort to issues involving basic freedoms like privacy. These cost/benefit tradeoffs have to be considered when undertaking security investments. Typically the benefits of information security investments will initially increase but may eventually reduce since the probability of breach will reduce as level of information security investments increase. The cost of information on the other hand may initially increase slowly but may increase at a higher rate due to access restriction placed by more controls at higher levels of secured IT environments.

4.1 Definition of Terms and Variables

i : Index for project[4]
s_i : Level of information security (expressed as an index) associated with project *i*
I_0 : Base level of information security investment cost
I_i : Information security investment cost associated with project *i*
$\hat{B}_i$: Benefit (cost savings) associated with preventing a security breach by investing in s_{i} level of information security
$\hat{C}_i$: Total information security related cost (excluding investment costs)
a_{0i} : Annual avoidable fixed operating costs pertaining to project *i*
a_{1i} : Variable cost per unit level of information security pertaining to project *i*
a_{2i} : Quadratic cost term reflecting increasing marginal cost per unit level of information security pertaining to project *i*
C_B : Cost of a security breach if no information security investment is made
$\Pr(o|s_i)$: Security breach probability function (probability that a breach will occur given a level of information security investment $\mathrm{s_i}$)
k : discount rate
r : risk-free rate
τ : corporate tax rate
$f(s_i)$: net annual after tax cash flows pertaining to project *i*

4.2 Level of Security Investment:

The investment cost associated with a security investment will include the hardware cost and one-time IT labor cost for configuration and system set up. We argue that the systems designers have the flexibility to configure the detection systems depending on how much they

[4] We use the term project and investment opportunity interchangeably to describe an investment in information security

wish to spend on system hardware and the labor costs. For example, one investment alternative may be to configure system at a low security level by not allocating much IT labor. Another alternative may be to allocate a higher level of IT labor to achieve a high level of security. There are two primary cost components associated with information security the *system configuration specific costs* and the *operating costs*. The costs and benefits of security investments are assumed to vary with the level of security investment denoted by s_i. In order to express the security investment costs as an index we use a base level of security investment (I_0). The level of information security is then given by:

$$s_i = \frac{I_i}{I_0} \qquad \text{----------------------(6)}$$

4.3 Benefit function:

The benefit function associated with the information security investment is the expected benefit of preventing a breach. It is a function of the level of information security and the probability of a breach occurring conditional on the level of security. The probability of a breach occurring is modeled by a decay function as $\Pr(o|s_i) = e^{-s_i}$. Then the probability of avoiding a breach is given by $1 - e^{-s_i}$, which is equal to the probability of detecting a breach for a given level of investment P_D^i . In Figure 5 below we show the probability breach function. For any level of investment s_i one can compute the probability of detecting P_D^i and using the ROC curves for a given $r_i = \frac{\lambda_F^i}{\lambda_N^i}$ we can compute the probability of false positive P_F^i. The assumption that quality parameters are a function of the money spent (resources allocated) on IT security is a reasonable assumption since that is exactly what happens in practice.

Given the probability of a breach, the benefit from preventing a breach can be calculated using the probability of avoiding the breach, the complement probability $(1 - e^{-s_i})$ times the cost of an information breach if no security investment is made. Therefore the benefit associated with preventing a breach is

$$\hat{B}_i = C_B(1 - \Pr(o|s_i)) = C_B(1 - e^{-s_i}) \qquad \text{-----------------------(7)}$$

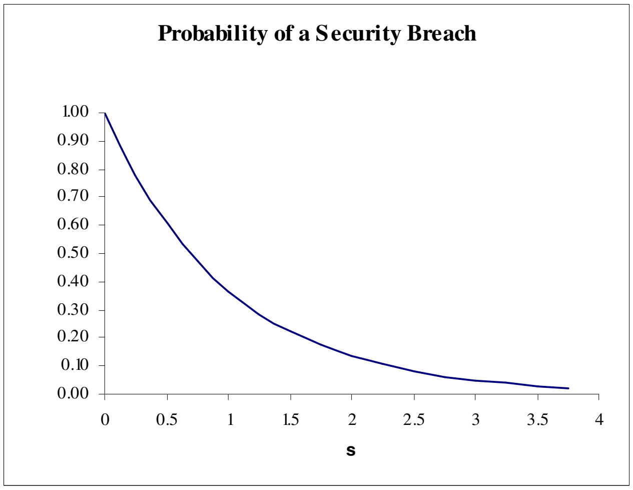

Figure 5. Security Breach Function

Notice that the function is independent of the time subscript indicating that the benefit associated with a certain level of investment will be the same throughout the project life. This is simplifying assumption and can be easily relaxed. The cost of a breach (C_B) is difficult to measure exactly due to unavailability of firm specific data. In order to overcome this difficulty we model C_B as a continuous random variable having a triangular (PERT type) distribution for Monte Carlo simulation.

4.4 Cost function:

The total cost function includes the configuration specific costs as given in Equation (5) for some level of investment s_i and the operation costs with annualized cost parameters. We consider the following as operating costs (annual fixed operating costs that can be avoided if the information security is not put in place). These are hiring costs of IT security personnel to maintain the system independent on the level of IT security capacity acquired. Second the annual variable portion of costs, which will depend on the level of information security investments such as training costs etc. Third, the opportunity cost associated with loss of site access as more and more controls are emphasized. We assume these costs to have a quadratic term so that the total cost of information security will initially increase at a decreasing rate and thereafter increase at an increasing rate due to access restriction place by higher levels of information security. The total cost function with configuration specific cost and operating costs are given below:

$$\hat{C}_i = \{cP_D^i\psi + d(1-P_D^i)\psi + c_1P_F^i(1-\psi)\} + \{a_{0i} + a_{1i}s_i + \frac{1}{2}a_{2i}s_i^2\} \text{ ---------------------(8)}$$

The annual after tax cash flow related to project *i* is given by

$$f(s_i) = (1-\tau)(\hat{B}_i - \hat{C}_i) \qquad \text{-----------(9)}$$

Where τ is the tax rate and $\hat{B}_i$ and $\hat{C}_i$ are as in Equations 7 and 8 respectively. Assume that each project has an economic life of 3 years, and the cost of capital is k . Then the net present value NPV of project i is given by

$$\text{NPV}(i) = (1-\tau)(\hat{B}_i - \hat{C}_i)(P/A, k\%, 3) - I_i$$

where, $(P/A, k\%, 3)$ is the present value of annuity factor. Then as in Figure 6 we can pick the configuration that provides the highest NPV, given IT budget constraints.

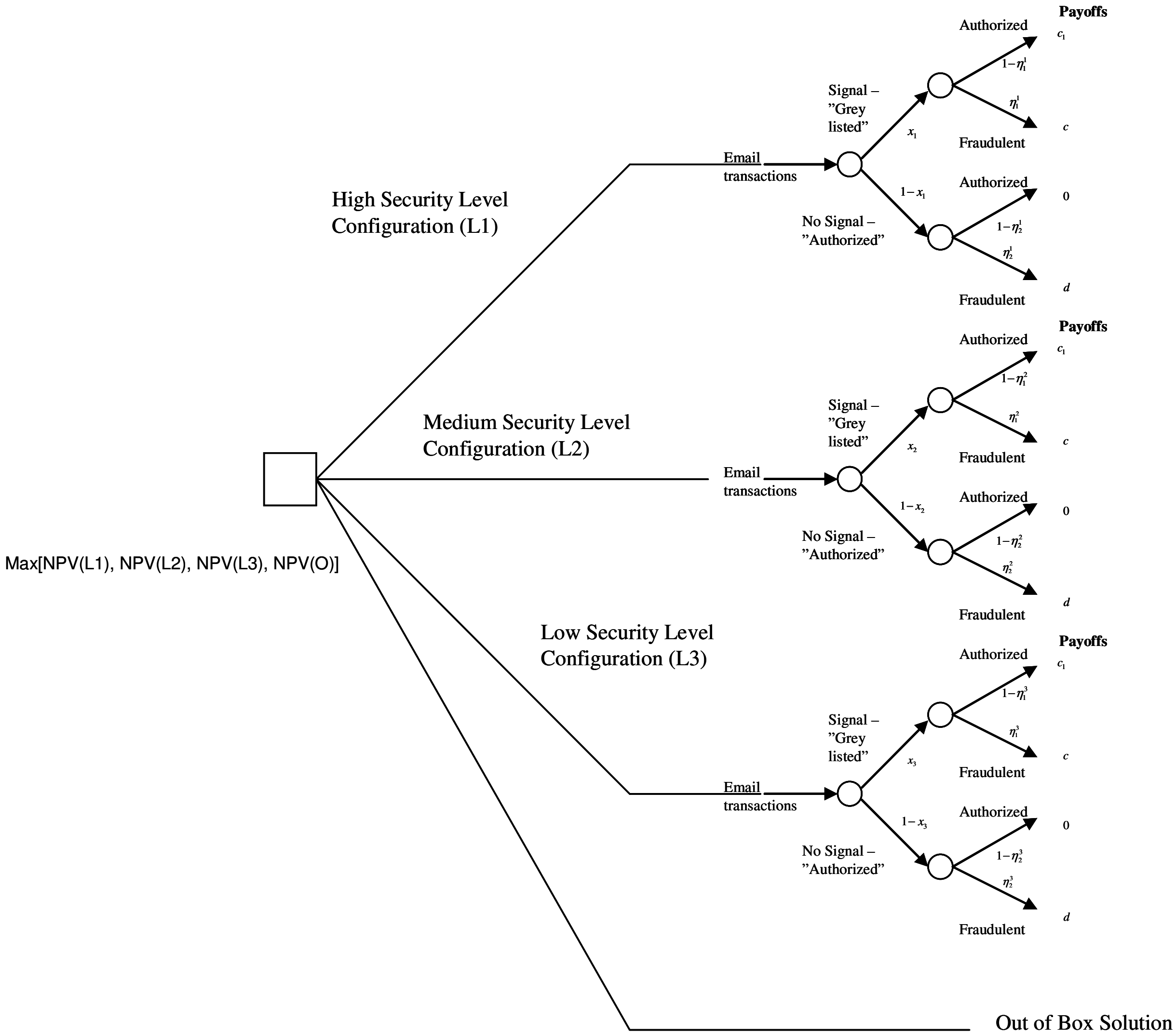

Figure 6. Decision Tree for Investment Options

5. Model Application

We illustrate the application of the model using the actual data for NAU’s email transactions for the 1st September 2005 to 15th February 2006 period given in Table 3. The parameter values related to NAU’s investment alternatives, option I (low level of security configuration), option II (medium level of security configuration), option III (high level of security configuration) and option IV (off-the shelf box) are given in Table 4. We make the following assumptions: NAU’s IT budget is limited to $50,000, each investment alternative (option I, II, and III) have project life of three years, and to find the level of security (s_i), we assume a base level of investment (I_0 = $100,000). The probability of a detection is computed as $P_D = (1 - e^{-s_i})$.

Table 3. NAU's Email statistics for
1st September 2005 to 15th February 2006

Outgoing	2203200
Incoming	8639741
Total e-mail transactions	**10842941**
Incoming	
Virus	5180
Spam	138536
Reject	2821683
Longform User	421843
Grey	1582794
Triplet (White, Black, New) and Misc	1942814
Passed	366259
Accepted	454860
Mail in	905772

The ratio of mean score of normal transactions to that of fraudulent transactions $r = \frac{\lambda_F}{\lambda_N}$ is determined by defining *normal transactions* as "# of passed" + "# of accepted" + "# of mail in" and *fraudulent transactions* as "# of viruses" + "# of spam" + "# of reject". We assume a constant r for illustration simplicity but this can be relaxed. Next from the ROC curves we compute the probability of false positive P_F . The proportion of malicious emails ψ is found by dividing the # of fraudulent transactions (computed as "# of viruses" + "# of spam" + "# of reject") by the total # of "incoming mail".

Since the benefit and cost parameters are difficult to precisely estimate we recommend using Monte Carlo simulation. For each of the three alternatives we assume the following benefit and cost input parameters[5]. The cost of security breach (*C_B*) is modeled by a triangular distribution with minimum security breach cost of \$150,000, a modal value of \$170,000 and a maximum security breach cost of \$215,000 i.e. T[150,170,215] in thousands. For the configuration specific cost parameters we assume the following: annual investigation cost of correctly signaled malicious email to be uniformly distributed over the interval c~[\$10,000, \$15,000] i.e. opportunity cost plus cost to investigate an incorrectly signaled email as c_1 ~U[\$12,000, \$17,000], damage from an undetected email, virus d ~U[\$20,000, \$80,000]..

The following operating costs parameters are assumed; an annual fixed cost to be uniformly distributed over the interval [\$7,000, \$12,500] i.e. a_{i0} ~U[7, 12.5] in thousands, the variable cost per unit level of investment uniformly distributed over [\$1,000, \$2,500] i.e. a_{i1} ~U[1,2.5] in thousands and the marginal cost per unit level of information uniform over the interval [\$500, \$800], i.e. a_{i2}~U[0.5.0.8] in thousands. The data for the three projects is summarized in Table 4. A company's cost of capital of 10% per annum is assumed, reflecting a risk-premium of 3% above the risk-free rate of 7%. The marginal tax is assumed to be 40%.

Table 4: Cost and Parameter Values

All costs are in thousands of \$

Description	**Option I**	**Option II**	**Option III**	**Option VI**
Project life	3 years	3 years	3 years	
Investment cost (I_i)	\$35	\$50	\$59	\$45
Level of investment (s_i)	0.35	0.50	0.59	0.45
P_D	0.29	0.39	0.45	0.36
P_F	0.49	0.58	0.62	
r	1.72	1.72	1.72	
ψ	0.343	0.343	0.343	
Cost of a security breach (C_B)	T[50,70,115]	T[50,70,115]	T[50,70,115]	
Annual fixed (a_{i0})	U[7, 12.5]	U[7, 12.5]	U[7, 12.5]	
Variable cost (a_{i1})	U[1,2.5]	U[1,2.5]	U[1,2.5]	
Marginal cost (a_{i2})	U[0.5.0.8]	U[0.5.0.8]	U[0.5.0.8]	

[5] We have assumed the same costs and benefit parameters for all the three projects for simplicity but different values can be considered for each project.

c	U[10, 15]	U[10, 15]	U[10, 15]	
c_1	U[12, 17]	U[12, 17]	U[12, 17]	
d	U[20, 80]	U[20, 80]	U[20, 80]	

6. Conclusions

In Table 5, we present the simulation output for each of the three IT security investment alternatives along with the out-of-the-box alternative. Since NAU's IT security budget is limited to $50,000, option III is not viable although it has the largest NPV. From the remaining two in house configuration alternatives, option I will be rejected as the NPV is negative. Then the best in house configures alternative is option II with a positive NPV and a high profitability index. Since NAU can also buy an out-of-the-box system for $45,000, there are two possible IT security investment alternatives: (1) select a medium security level configuration (option II) or (2) the out of box alternative (option VI). NAU decided on option II since the probability of detection is higher than under option (IV). Other factors favoring option II include greater flexibility to manage since IT staff are familiar with the configuration as it was developed in house, value of learning, and in house training.

Table 5. Summary of Results

	Opion I	Option II	Option III	Option VI
Mean(NPV)	(12,646)	21,511	21,874	
stdev(NPV)	6,489	8,129	9,313	
Investment	35000	50000	59000	45000
Profitability index	0.64	1.43	1.37	
prob of detection	0.295	0.393	0.446	0.362

In this article we investigated the spam email and virus problem of an organization and demonstrated how theoretical research can be applied in practice through a real life case study. Future research should also look at how game theoretic models can be incorporated into this framework in a multi-period setting if hacking is found to be significant. Although, we have considered the viability of several configuration alternatives, we have not investigated the managerial flexibility or embedded real options to choose on the optimal timing of investment.

Acknowledgement

We would like to thank computing consultants Josh Sekel and Shawn Marriott for their valuable input.

REFERENCES

2004. *2004 E-Crime Watch Survey Summary of Findings*. Retrieved December 3, 2004, from Computer Emergency Response Team Coordination Center Web Site: http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf

Cagnemi, M. P. 2001. Top Technology Issues. *Information Systems Controls Journal*, 4(6).

Camp, L. J., C. Wolfram. 2004. Pricing Security. J. Camp and R. Lewis (eds). *Economics of Information Security*, Kluwer, 17-34.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2005. The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, 16(1), 28-46.

Cavusoglu, H. 2004. Economics of IT Security: A Literature Review. J. Camp and R. Lewis (eds), *Economics of Information Security*, Kluwer, 71-84.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2004. A Model for Evaluating IT Security Investments. *Communications of ACM*, 47(7), 87-92.

Cavusoglu, H., S. Raghunathan. 2004. Configuration of Detection Software: A comparison of Decision and Game Theory Approaches. *Decision Analysis*. 1(3), 131-148.

CSI/FBI. 2004. *2004 Computer Crime and Security Survey*. Retrieved September 12, 2004, from http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

Gordon, L. A., M. P. Loeb, W. Lucyshyn. 2003. Information Security Expenditures and Real Options: A Wait and See Approach. *Computer Security Journal*, 19(2), 1-7.

Gordon, L. A., M. P. Loeb. 2002. The Economics of Information Security Investment, *ACM Transactions on Information and Systems Security*, November, 438-457.

Hoo, K.J. Soo. 2000. How much is Enough? A Risk Management Approach to Computer Security. Consortium for Research on Information Security Policy (CRISP) Working Paper, Stanford University, June.

ICSA Labs. 2004. Computer Virus Prevalence Survey.

Longstaff, T.A., C. Chittister, R. Pethia, Y.Y. Haimes. 2000. Are we forgetting the Risks of Information Technology? *IEEE Computer*, December, 43-51.

Ulvila, J.W., J.E. Gaffney. 2004. A Decision Analysis Method for Evaluating Computer Intrusion Detection Systems. *Decision Analysis*. 1(1) 35-50.