Return on Information Security Investment

The viability of an anti-spam solution in a wireless environment

Adrian Mizzi, June 2005

e-mail: amz@yahoo.com

Abstract

Much is said about the importance of investing in information security (Potter 2004; Ernst & Young 2003), but little is known on the extent and effectiveness of such security programmes (Cosgrove Ware 2004). A model that analyses the mechanics of an information security programme is presented. The model attempts to put an upper-bound on the information security expenditure. The concepts of "viability of security expenditure", "successfulness of attack" and "motivation to attack" are introduced. The Return on Information Security Investment (ROISI) model is tested in a real life organisation to determine the viability of an anti-spam solution in a conventional setting and later adapted to a wireless environment.

Introduction

Organisations, large or small, that are undergoing electronic business (e-business) activities, have **information assets** that are susceptible to risk by virtue of the fact that the business is connected to third party networks, typically but not necessarily, via the Internet.

The information assets[1] consist of hardware and software components that are the fruit of the work of a plethora of suppliers, systems integrators and internal employees. The value of the *Information Assets* comprises *tangible* and *intangible* assets (Brykrzynski & Small 2003). The tangible component is the sum total of the cost to implement the various hardware and software elements of a system. The intangible component includes the *value* of the data stored in databases, the knowledge (Freese 2001) and the intellectual property stored within a system. The value of the intangible assets may be difficult to calculate in monetary terms.

Whatever architecture is used to build the information assets, it is common knowledge that part or all of these information assets are *more* **at risk** by virtue of them being in an electronic format and possibly connected to a local area network (LAN) and perhaps to a wide area network (WAN).

Security and Risk

Even when considering a standalone system that is not connected to any network, such as a computer maintaining the operations of a DVD rental store, there are inherent risks that may lead to data loss and ultimately loss of monetary value. If the computer hosting the DVD rental application develops a hard disk crash leading to system outage; then the *availability* of the system has been compromised – the system is down. Money spent to backup the system, on say a CD-ROM or a tape drive, is money spent on securing the system (from a holistic, not just from a hardware, perspective) from such failures. Were it not for the possibility of data loss, had we lived in a perfect world, this money would not have been spent.

If there is no mechanism restricting the usage of the DVD rental system, any person visiting the DVD shop can walk in and tamper with the system. Any money (or time!) spent in setting up and using password mechanisms that allow only the rightful owner to access the authorised part of the system is money spent to secure the *confidentiality* and *integrity* of the system.

The wide definition of **security** generally refers to the *Confidentiality*, *Integrity* and *Availability* of the information assets (Brykrzynski & Small 2003), and is often referred to as **CIA**.

[1] The term "*information assets*" is used in a wide sense within this context. In other contexts, the term "Information Technology (IT) system" may be encountered instead.

The same concepts apply when a computer is connected to any kind of network. This paper will provide the rationale needed to understand the expenditure required even in the smallest of information technology systems, that is, stand-alone systems that are not connected to a network. Hence the use of the term *information assets*, rather than *e-business infrastructure*, that may be used in other literature.

Vulnerabilities

As previously discussed, then, there may be inherent vulnerabilities even in the case of a standalone system. The availability 'vulnerability' brought about by a hard disk failure has already been pointed out. Likewise, loss of information may be brought about by data corruption, if, for instance, the underlying operating system malfunctions. Also, any person accessing the system without authorisation by, say, guessing a password, may compromise the integrity of the system by modifying the outstanding payments on his or her account or making other fraudulent changes.

However, if that person instead spies on what DVDs his or her neighbour has rented, he or she will have compromised the confidentiality of the system. Confidentiality and integrity vulnerabilities become more pronounced when computers are connected to a network. The area of vulnerability-finding is still in its infancy and, according to (Rescorla 2004), the evidence that the effort being spent on vulnerability-finding is well spent, is weak.

Information Assets at Stake

Depending on the topology of the network, some portions of the IT assets may be more susceptible to having their vulnerabilities exploited. Typically, an organisation will implement an internal LAN, a demilitarised zone (DMZ) and an Internet segment. The LAN is usually protected with **defence mechanisms**, such as Internet firewalls and Intrusion Detection Systems (IDS). However, internal protection is typically scarce, and it is thus more susceptible to attacks from internal employees than from attacks coming from the Internet segment. The subject of **information assets at stake** is now introduced, namely the portion of the information assets that can be breached by virtue of them possibly having vulnerabilities or by incorrect usage of the system by authorised users, typically employees.

Security Expenditure

The IT department will over time purchase licences and in general spend money to fix system vulnerabilities, as these are made available by the suppliers of the components of the system. The variable [F] is defined as the annual cost to fix vulnerabilities by the application of system patches or upgrades to the system containing the information assets at stake, Figure 1.

A company will typically spend a one time cost [B] to implement defence mechanisms that protect IT assets from possible threats. It will most probably incur an annual maintenance cost [M], not shown in Figure 1, to cover for upgrades and updates of the defence mechanisms.

The total annual security expenditure [E_S], for the first year, of an organisation is given by

$$\mathbf{E_S = F + B + M} \qquad \mathbf{[1]}$$

In subsequent years the organisation spends a total of

$$\mathbf{E_S = F + M} \qquad \mathbf{[2]}$$

Loss of Revenue

Whenever a system is exploited, there is a probability that there is an **immediate loss of revenue,** [L] that is brought about by the exploit; be it by system outages, third parties or internal employees. Typically[2], a few seconds after a security incident, there will be an outage that may be detected and reported to the relevant IT personnel to intervene. During the outage there is the possibility of loss of new revenue brought about by the fact that the "system is down". The DVD rental shop may lose the opportunity to rent DVDs to clients until the system is repaired. Likewise if data is stolen or tampered with, the system will have incurred confidentiality and integrity loss.

Two components of the loss are shown to exist. The first is a function of the time [t] that the

[2] Historically there were several instances when attacks went undetected. Recently an attack on MSN went undetected for several days according to (Bridis 2005).

system was down and the second is the lump sum of money, L_I that is lost *immediately*. For the scope of this paper it is assumed that the variable loss is a fraction of the value of the information assets at stake, which is quoted annually[3].

Total Loss

A variable, L_T (Total Annual Loss) is defined such that

$$\mathbf{L_T=L_I+I*t/365} \qquad [3]$$

where, L_I is the instantaneous loss, I is the value of the information assets at stake, t is the time, in days, that the system is unavailable for service. Organisations can also model the loss differently as A(t), availability loss[4], a function that describes the way that the revenue of the information assets at stake is lost over the time period, t, during which there is an outage. Thus, more generally:

$$\mathbf{L_T = L_I + A(t)} \qquad [4]$$

Subsequent to the incident, and during the time that information is being lost or new revenue not being made, IT personnel will be attempting to fix the system, either by restoring from backups or replacing equipment, or by performing any operation to restore the system to the original state. Whatever the method chosen, there is a financial cost to rebuild [R] the system attached to such an operation and hence [3] is modified to

$$\mathbf{L_T = L_I + A(t) + R} \qquad [5]$$

Frequently, the man-hour labour cost [R] will be the dominant cost, and hence [4] may be rewritten as

$$\mathbf{L_T = L_I + A(t) + R(t)} \qquad [6]$$

where [R(t)] is a function describing the annual money spent to rebuild lost IT assets during the time that the system was down.

Frequently the length of time (t) during which the system can be reasonably expected to be down will be dictated by the service level agreement (SLA) of the organisation in question. Typically, the lower t is, the more the company will have paid for the corresponding SLA. Possibly part of the expenditure in R(t) is money that was spent in the SLA, if this is provided by a third party organisation and not by internal personnel.

Viability of Expenditure

The objective of any information security programme is to protect the information assets in a cost effective way. Moreover, the **defence mechanisms** should not themselves compromise the availability of the system by introducing extra points of failure.

Figure 1 depicts the components outlined so far and poses the question as to the viability of the security investment that is given algebraically by combining [1] and [6]. The security project is viable if

$$\mathbf{E_S < L_T} \qquad [7]$$

Or alternatively,

$$\mathbf{(F + B + M) < (L_T + A(t) + r(t))} \qquad [8]$$

This is in agreement with (Gordon 2004), who argues that “an organisation should spend substantially less than the expected loss, no more than one third”.

Cost to Break

The analysis presented so far focused on the vulnerabilities intrinsic to the system. The possibility of an attack was not factored in. A system not protected by defence mechanisms and having numerous vulnerabilities is still not in danger of being damaged if there are no threats. To complete the model the notion of threats is introduced.

The first threat is to the defence mechanisms themselves. Denial of Service and other attacks on external routers and firewalls that may knock the defence mechanisms themselves, without

[3] Possibly this might be quoted under the section of “intangible assets” in the balance sheet of the organisation.

[4] A(t) = I * t / 365 assumes that the loss is uniform over time. This is a rough approximation. In practice the organisation will have to find an approximation to A(t) depending on the setup in question.

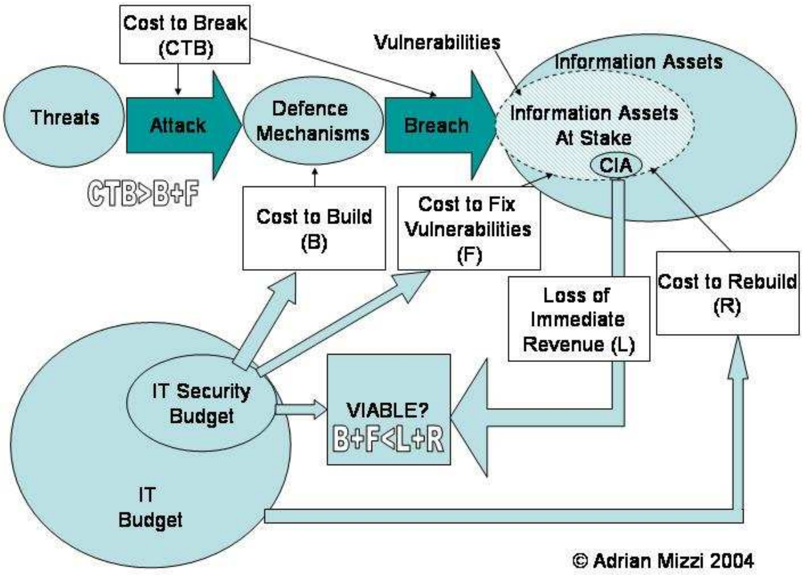

Figure 1 Viability of an Information Security Investment

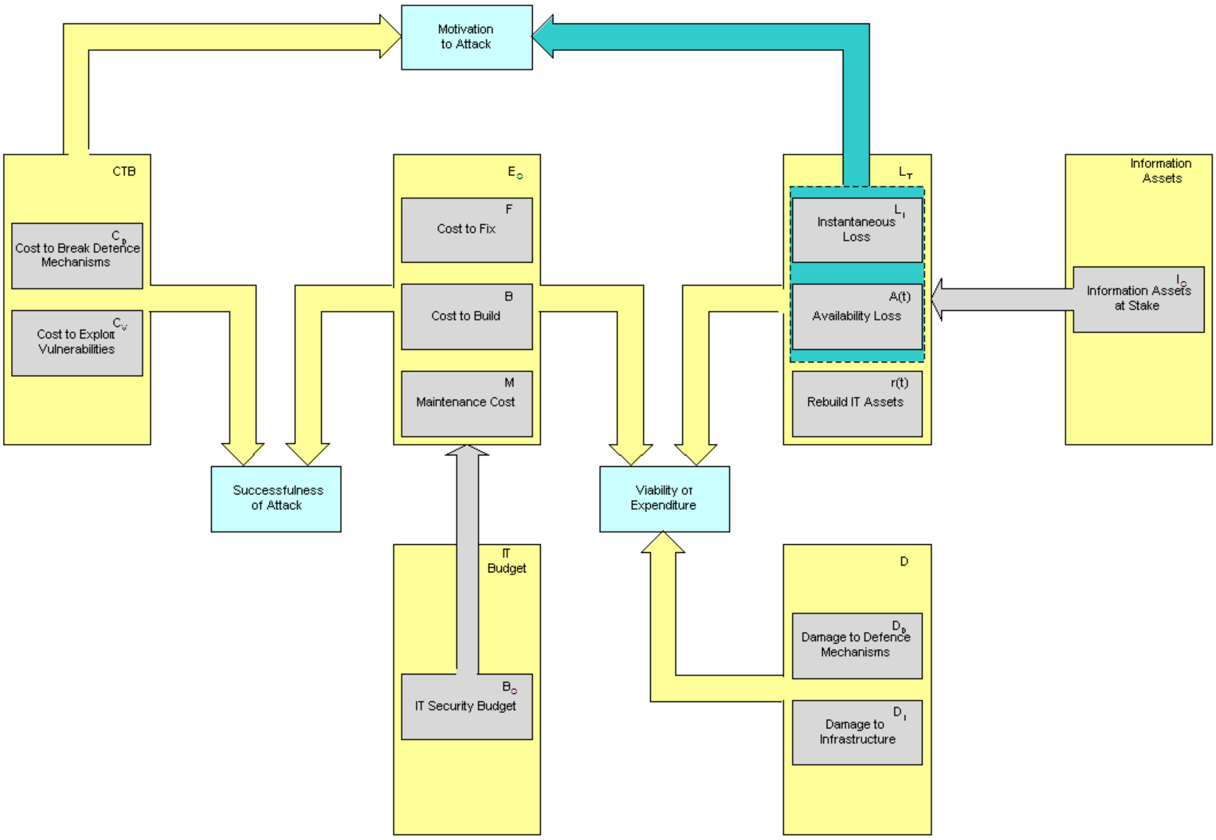

Figure 2 Detailed ROISI model

necessarily compromising the IT assets, may be attempted. Furthermore, the attack may propagate to exploit the vulnerabilities in the defence mechanisms. A variable Annual Cost to Break [CTB], is defined such that

$$\mathbf{CTB = C_D + C_V} \qquad \mathbf{[9]}$$

where C_D is the annual cost to break into the defence mechanisms and C_V is the annual cost to exploit vulnerabilities in the system. It is appreciated that this figure is very hard to calculate. (Schechter 2002) suggests that organisations employ personnel to attempt to break into the system to obtain a value of this figure. A theoretical upper-bound of CTB is given later on in this paper.

Damage to Defence Mechanisms

Corresponding annual damage [D] is done to the systems by the attack on both the defence mechanisms [D_D] and the underlying infrastructure [D_I] that *hosts* the information assets but not the information assets themselves. This damage does not necessarily result into information loss, but will have to be repaired just the same. The cost to repair is thus denoted by

$$\mathbf{D = D_D + D_I} \qquad \mathbf{[10]}$$

D_D and D_I are in fact probabilistic functions (not shown in Figure 2).

The inequality given in [8] may be modified such that the information security project is viable if:

$$\mathbf{(F + B + M) < (L + A(t) + r(t) + D)} \qquad \mathbf{[11]}$$

Successfulness of an Attack

It is assumed that in a well-informed society[5], a hacker or other malicious user will not manage to break or abuse a system unless he spends more than what it costs to build the defence mechanisms[6]. Thus the defence mechanisms should be built such that the cost to break is more than what it costs to build them. Thus for a well designed system:

$$\mathbf{CTB > (F + B + M)} \qquad \mathbf{[12]}$$

Motivation to Attack

Likewise, in a well informed society, a malicious entity is expected to be typically prepared to pay close to, but not more than, the instantaneous loss [L_I], if it intends to steal data or possibly L_I+A(t) if it intends to damage an organisation's reputation. This will give an indication of the CTB, such that typically there is a motivation to attack the system if

$$\mathbf{CTB < (L_I + A(t))} \qquad \mathbf{[13]}$$

The perception of information value for the attacker may be in fact greater than the perception of value of the information owner, in which case motivation may still remain high even with a high CTB.

ROI, ROSI and ROISI

This paper introduces the term "Return on Information Security Investment" (ROISI), that is a build-up on the terms Return on Investment (ROI), and Return on Security Investment (ROSI) that are commonly used. The use of the term ROISI is intended to distinguish the methodology used in this paper from that found in the literature and encompasses the concepts of ROI and ROSI, whilst emphasising on "Information". The word ROISI is used interchangeably with ROI to emphasise the use of the ROISI model in the calculation of traditional ROI percentages later on in this paper.

The ROISI Model

The Return on Information Security Investment Model (ROISI), shown in Figure 2 illustrates the relationship between the variables discussed in this paper and highlights the importance of obtaining estimates of the quantities labelled by "Viability of Expenditure", "Motivation to Attack" and "Successfulness of an Attack".

[5] With the globalisation that is taking place in today's world it is assumed that the security practitioner and the attacker are equally informed about the technology used to build the defence mechanisms.

[6] It is assumed that the defence mechanisms are well configured. Negligence and wrong configuration of equipment might lead to the demise of the most expensive of defence mechanisms.

Perhaps the most important quantity is the "Viability of Expenditure" which would then be followed by studying the values obtained by the other two quantities. The following section illustrates how the model can be used in practice. Organisations should adopt the model and adapt it to their circumstances by defining relationships among the variables according to the nature of their organisation.

ROISI Model in Practice

The model was tested in a real organisation (c. 250 employees), located in Malta, that was considering investing in an anti-spam solution. It was unclear what the benefits of anti-spam solution would be. The IT department was hesitating to implement an anti-spam solution, claiming that "there is no need to implement anti-spam techniques". On the other hand users were complaining that they were being bombarded by spam. This led the organisation to allocate LM4,000[7] to research and implement an anti-spam solution.

The organisation in question decided to use the method suggested in this paper to rationalise the debate and to determine whether to invest in anti-spam technology. The research was done following the outbreak of the Sober.q worm (Pruitt 2005) that occurred in the week 12-19 May 2005 and that became known as the "German spam".

This intentional bias was introduced so as to obtain an upper limit of the estimated losses. In practice the problem of spam would not be as acute. The rationale employed was that if the project was not viable with these figures, then it would be even *less viable* with *less-inflated* figures. This approach may be subject to debate: other organisations may want to adopt a different methodology and measure the variable that quantifies the losses under normal conditions.

A questionnaire was sent to 168 of the 250 total users who were asked to specify the amount of time they spend dealing with spam email. The questionnaire was successfully filled in by 46% of the population.

The results are summarised in Figure 3. As can be seen, users spend an average of 3 minutes per day dealing with spam, which they receive at the rate of 8 spam emails per day. On average users spend 31 minutes per day reading e-mail (including the time spent dealing with spam itself). This is significantly less than the 1 hour 47 minutes reported by the (American Management Association 2003).

96% of respondents spend less than 10 minutes per day dealing with spam e-mail. This is considerably more than the 60% that spend less than 14 minutes per day that is mentioned in a similar study by (Fallows 2003).

The questionnaire also sought to determine the way that users deal with spam. This data would be used by the IT department to determine the right anti-spam product that would best fit the needs of the organisation. The data is beyond the scope of this paper and is not shown here.

Time Spent Dealing with Spam (minutes per day)	3.3
Average Number of Spam e-mail received (per day)	8.1
Total Time Spent Reading e-mail (minutes per day)	31.3

Figure 3 Summary of Results of Survey to obtain an estimate for the Time Spent Dealing with Spam in the Organisation under study (N=78).

Total Loss (Actual Data)

The results from the questionnaire, together with the average size of spam e-mail (8KB), average salary per employee and the cost of storage of an e-mail system were used to determine the values of the variables A(t), and D_I. Interviews with IT personnel were carried out to determine the time lost by IT employees which helped to determine the value of r(t). In practice, an organisation may opt to use approximations to determine the value of the variables as suggested in this paper.

The values of the following variables were determined:

L_I=LM600;

A(t)=LM9,750;

r(t)=LM2,000;

D_I = LM99; and

D_D = 0

[7] The currency used throughout is Maltese Liri (LM). LM1 is approximately 2.8USD or 2.3Euros.

The total loss L_T was thus estimated by using the formula

$$L_T = L_I + A(t) + r(t) + D$$

$$L_T = LM(600 + 9{,}750 + 2{,}000 + 99)$$

$$L_T = LM12{,}449$$

Thus for the investment in an anti-spam solution, E_S, to be viable;

$$E_S < LM12{,}449$$

The proposed budget (E_S) of LM4,000 satisfies inequality [6] mentioned previously, and hence the investment is viable. In this case, the intuition of the IT department (assigning a budget of LM4,000) would have sufficed. However it is relatively easy to understand that had the organisation employed 25 employees instead of 250, then inequality [6] would have worked out to

$$E_S > LM1{,}250$$

and the stipulated LM4,000 budget would have been an overshoot and the investment would not have been viable.

Viability of Expenditure (Actual Data)

If the organisation manages to successfully implement an anti-spam system with a LM4,000 budget, then the organisation would be better off by LM12,350 less LM4,000; or LM8,350 per annum. The Return on Investment (ROI) for one year is 67%.

The next step is to verify the assumption that there exists an anti-spam solution that would cater for the needs of an organisation. At the time of writing an anti-spam solution may be obtained for less than LM1500. The ROI is thus adjusted to 86%.

This gives a value for the variable [B]. The chosen product has no maintenance cost [M]. It is assumed that once the system is installed there is negligible time spent by IT staff to fix problems [F]. This leads to:

$$F+B+M = LM1{,}500$$

Successfulness of an attack (Actual Data)

As denoted by inequality [11], a well designed anti-spam system should have a CTB > LM1,500. A simple calculation illustrates that this is indeed so. The organisation is estimated to receive 750,000 emails per annum. This amounts to 0.2 cents per spam e-mail received. It is estimated that spammers spend 5c per email sent (Ostrom & Langberg 2002). Thus a spam solution that costs LM1,500 would deter spam that costs LM37,500. It is to be noted that in practice the cost of spam is less than that quoted by (Ostrom & Langberg 2002) due to the fact that spam generated by self-replicating code is included in the total amount of spam in this study.

Motivation to Attack (Actual Data)

Using inequality [12] and the values for

$$CTB=LM37{,}500$$

$$L_I + A(t) = LM10{,}350;$$

then it can be seen that inequality [12] is not satisfied and thus there is no motivation to attack. It is to be noted however that spam is not normally associated with Denial of Service (DOS) attacks and the applicability of these figures may be questionable.

The Case of a Wireless Solution

Having established a framework that assesses the magnitude of the spam problem in the organisation under study, it is now relatively easy to take into account the case of an organisation that plans to offer a wireless solution to its employees. It is assumed that the organisation will deploy a wireless mobile solution that is provided by a mobile operator.

Typically mobile e-mail solutions may consist of a device that accesses the network via Short Message System (SMS), Circuit Switched Data (CSD), Wireless LAN (WLAN) or General Packet Radio Service (GPRS). The organisation will be charged by the wireless operator on either a duration or volume or a per message (count) basis as shown in Figure 4. The operator will charge the organisation on one of the following schemes. In the case of GPRS, for example, the organisation will be billed for 6GB of data, whereas if employees access the network via a Public WLAN (PWLAN) the organisation will be charged for 300,000 minutes of use.

Annual Billable Part of spam e-mail			
	Count	**Volume(KB)**	**Duration(min)**
CSD	-	-	300,000
GPRS	-	6,000,000	-
WLAN	-	-	300,000
SMS	750,000	-	-

Figure 4 The billable element of spam e-mail for a 250-employee organisation using different wireless technologies. SMS e-mail notification is assumed.

Cost of spam e-mail over Wireless				
	SMS	**GPRS**	**WLAN**	**CSD**
Unit Cost (cents)	2	0.2	4	10
Billable Amount	750,000	6,000,000	300,000	300,000
Total Cost (LM)	15,000	12,000	12,000	30,000

Figure 5 The total additional cost of spam e-mail for a 250-employee organisation using different wireless technologies (quoting current market prices in Maltese Liri)

Using the results shown in Figure 3, the extra cost, other than time lost, that the organisation would have to pay for the four methods of connection, due to bearer charges that are possible today is calculated in Figure 5.

Assuming that the organisation uses a combination of access technologies, additional expenditure may range from LM12,000 to LM30,000, or an average of LM17,000. The value of L_T will be significantly changed; and hence the anti-spam solution will be viable if:

E_S<Lm29,500

With a budgeted Lm4,000, the ROISI is 86%, whereas with a typical solution of Lm1,500, the ROISI works out to 95%.

	Conventional	Wireless
Budgeted	67%	86%
Actual	88%	95%

Figure 6 ROISI (1 year) for an anti-spam solution for a wired and a wireless solution

The ROISI for the actual solution is compared with that for the budgeted solution for the case of a conventional and a wireless system in Figure 6.

Organisations may want to extend the analysis using Net Present Value (NPV) or Internal Rate of Return (IRR) methods so as to calculate the viability of the project over a number of years. In this case, it is futile to continue the analysis because the project is viable in the 1st year of implementation as shown in Figure 6.

Further Research

The ROISI model introduced the concepts of “Motivation to Attack”, “Successfulness of an Attack” and “Viability of Expenditure”. These concepts form a triad, represented by the various inequalities that were presented. In this paper, the focus was on “viability of expenditure” as the name of the paper suggests. Further research on the “motivation to attack” and “successfulness of an attack” could be carried out. This would require a more detailed analysis of the security problem and the security solution in question.

In the presented case, the paper relies on the specifications presented by the anti-spam software supplier. Organisations may want to “challenge” these specifications and for instance conduct research to calculate the number of false positives and false negatives to get a better indication of the “successfulness of attack”. Similarly, other researchers might want to investigate the “motivation to attack” by conducting interviews with “spammers” to understand the “real” motivation behind spam, rather than relying on published data as was done in this case study.

Conclusion

An organisation should not spend more on its information security than the total cost of the portion of information assets that may be lost via an incident of any type. In a well-informed society a malicious user is not expected to spend more than it costs to build the defence mechanisms, but may be prepared to spend less than and possibly close to the value of the information loss that would be incurred by an organisation.

It was demonstrated that for the organisation under study, an anti-spam solution, at current market prices, would offer a positive return on information security investment (88%). A better ROISI (95%) will be obtained if the organisation plans to deploy wireless access technology for its employees.

However, had the organisation employed fewer employees, as is the case in most small and medium sized enterprises (SME) there might have been a negative ROISI and the company would have been better off without an anti-spam solution

References

American Management Association 2003, *2003 E-Mail Rules, Policies and Practices Survey*, Available: [http://www.epolicyinstitute.com/survey/survey.pdf] (31 May 2005).

Bridis, T. 2005, *MSN Site Hacking Went Undetected for Days*, Available: [http://security.ittoolbox.com/news/dispnews.asp?i=129900] (6 June 2005).

Brykrzynski, B. & Small, B. 2003, 'Securing Your Organization's Information Assets', *CrossTalk. The Journal of Defense Software Engineering*, vol. 16, no. 5, pp. 12-16.

Cosgrove Ware, L. 2004, *The State of Information Security, 2004*, Available: [http://www.csoonline.com/csoresearch/report75.html] (6 June 2005).

Ernst & Young 2003, *Global Information Security Survey 2003*.

Fallows, D. 2003, *Spam - How It Is Hurting Email and Degrading Life on the Internet*, Available: [http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf] (24 May 2005).

Freese, E. 2001, 'Harvesting Knowledge from the Organization's Information Assets', in *XML Europe 2001*, Isogen International, St. Paul, Minnesota.

Gordon, L. A. 2004, 'Economic Aspects of Information Security in a Netcentric World', in *SecurE-Biz CxO Security Summit*, Washington, D.C.

Ostrom, M. A. & Langberg, M. 2002, *E-mail users plagued by a rising tide of junk as senders grow bolder*, Available: [http://www.mercurynews.com/mld/mercurynews/news/special_packages/3107291.htm] (31 May, 2005).

Potter, C. 2004, *Information security - Security conscious*, Available: [http://www.financialdirector.co.uk/features/1137126] (15 January 2005).

Pruitt, S. 2005, *Latest Sober worm sends German spam*, Available: [http://www.networkworld.com/news/2005/051605-soberworm.html] (22 May 2005).

Rescorla, E. 2004, 'Is finding security holes a good idea?' in *Annual Workshop on Economics and Information Security*, 3 edn, University of Minnesota, MN.

Schechter, S. 2002, 'Quantitatively Differentiating System Security', in *Workshop on Economics and Information Security*, 1 edn, University of California, Berkeley.