Return on Information Security Investment

Are you spending enough? Are you spending too much?

Adrian Mizzi, January 2005

e-mail: amz@yahoo.com

Abstract

Much is said on 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. A model that analyses the mechanics of an information security programme is presented and will serve as the founding work of future research in this area. The model attempts to put an upper-bound on the amount that should be spent on an information security programme and estimates the amount an attacker is likely to spend to break into a system depending on the information assets at stake of the organisation in question.

Introduction

Organisations, large or small, that are undergoing electronic business[1] (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[2] will 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* will be made up of *tangible* and *intangible* parts (Brykrzynski & Small 2003). The tangible parts are the sum total of the cost to implement the various hardware and software elements of a system. The intangible parts include the *value* of the data stored in databases, the knowledge (Freese 2001) and the intellectual property stored within a system, and 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 stake** 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

[1] The subject of what constitutes e-business will be revisited it the section “E-business and Networking” in this paper.

[2] 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.

any network, such as a computer maintaining the operations of a video rental store, there are inherent risks that may lead to data loss and ultimately loss of monetary value. If the computer hosting the video 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 a 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 video rental system, any person visiting the video 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,** then, generally refers to the *Confidentiality*, *Integrity* and *Availability* of the information assets(Brykrzynski & Small 2003), and is often referred to as **CIA**.

E-business and Networking

The same concepts apply when a computer is connected to any kind of network. The term e-business is a rather vague term that has several connotations, typically implying that a company is engaged *in doing business with other organisations or individuals in an electronic fashion*. Loosely speaking, then, an e-business will include at least one computer connected to any network in order to do business.

Under such a definition, the stand alone computer running the operations of a video rental system may not classify as an e-business system. Nevertheless, this paper will provide the rationale needed to understand the expenditure required even in the smallest of information technology systems; hence the use of the term information assets, rather than e-business infrastructure or other terminology, that may be used in another similar contexts.

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 videos 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 the computers get 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.

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] to cover for upgrades and updates of the defence mechanisms.

The total annual security expenditure [E_S] of an organisation is given by

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

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[3], 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 video rental shop will be handicapped and possibly may lose the opportunity to rent videos to clients until the system is repaired. Likewise if data is stolen or tampered with, then 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 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[4].

Total Loss

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

[3] There were several instances when attacks went undetected.

[4] Possibly this might be quoted under the section of "intangible assets" in the balance sheet of the organisation.

$$\mathbf{L_T = L_I + I * t/365} \qquad [2]$$

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[5], 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:

$$\mathbf{L_T = L_I + A(t)} \qquad [3]$$

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 in general doing 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

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

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

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

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 failures, which would otherwise have been avoided.

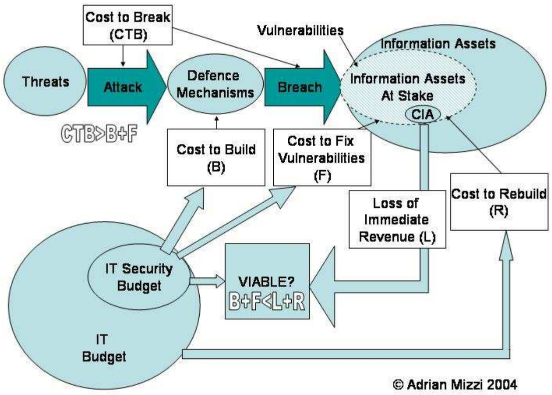

Figure 1 Viability of an Information Security Investment

Figure 1 depicts the components outlined in the ensuing discussion and poses the question as to the viability of the security investment that is given algebraically by combining [1] and [5]. The security project is viable if

[5] 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.

$$\mathbf{E_S < L_T} \quad \mathbf{[6]}$$

Or alternatively,

$$\mathbf{(F + B + M) < (L_T + A(t) + r(t))} \quad \mathbf{[7]}$$

According to (Gordon 2004), an organisation should spend substantially less than the expected loss, no more than one third.

Cost to Break

The analysis presented so far was based on the vulnerabilities intrinsic to the system in question. 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 necessarily compromising the IT assets, may be attempted. Furthermore, the attack may propagate to exploit the defence mechanisms. A variable [CTB], Annual Cost to Break, is thus defined such that

$$\mathbf{CTB = C_D + C_V} \quad \mathbf{[8]}$$

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 and not the information itself. 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

$$\mathbf{D = D_D + D_I} \quad \mathbf{[9]}$$

The inequality given in [7] may be modified as follows: the project is viable if:

$$\mathbf{(F + B + M) < (L + I(t) + r(t) + D)} \ \mathbf{[10]}$$

Successfulness of an Attack

It is assumed that in a well-informed society[6], 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[7]. 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:

$$\mathbf{CTB > (F + B + M)} \quad \mathbf{[11]}$$

[6] 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.

[7] 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.

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, L_I, if it intends to steal data or possibly $L_I+I(t)$ 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

$$\mathbf{CTB < (L_I + A(t))} \qquad \mathbf{[12]}$$

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.

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.

References

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.

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

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.

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