Managing Information Security in Modern Commercial Environments

Steve Purser

Steve Purser is Director ICSD Cross-Border Security Design and Administration at Clearstream Services, Luxembourg. Steve is also a founder Member of the "Club de Sécurité des Systèmes Informatiques au Luxembourg (CLUSSIL)" and author of « A Practical Guide to Managing Information Security (Artech House, 2004).

Introduction

The arrival of affordable and reliable network technology in the nineteen-nineties, followed by the move towards global connectivity and the success of the Internet as a medium for carrying out business, have drastically changed the way in which the modern enterprise operates. The positive aspects of this network revolution are difficult to overstate. Large international concerns have been able to make major efficiency gains, streamlining their operations and greatly reducing cost, whilst small and medium sized companies have benefited from the possibility of widening their markets to an international clientele. Last but not least, consumers have benefited from the ability to compare prices from disparate sources rapidly and to make purchases from their own home.

The effects of these events have not been limited to the way in which enterprises do business, but have had secondary effects on such diverse areas as organisational structure, the legal system and the way in which technology itself is evolving. Where information security is concerned, the move towards greater connectivity and the accompanying tendency to distribute processing over several platforms (possibly separated by geographical boundaries) has resulted in a number of issues that are still being resolved.

Despite the fact that most of these issues are well understood and considerable progress has been made in dealing with many of them, it remains a fact that there has been a significant growth in IT security-related risk over the last few years. The total number of security incidents recorded by the Computer Emergency Response Team (CERT) for instance rose from 2 412 in 1995 to 137 529 in 2003, representing an increase of 5 702 % [1]. Similarly, a comparison of data published in the 2002 CSI/FBI Computer Crime and Security Survey with data from the corresponding 2001 survey shows that 90% of respondents detected security breaches in 2002 (85% in the 2001 report) and 80% of respondents acknowledged financial loss due to computer breaches (64% in the 2001 report). Where financial loss could be quantified, this led to a total loss of $455,848,000 in 2002, as compared to $ 377,828,700 in 2001 [2,3].

It is therefore clear that companies need to better manage information security-related risk if they are to enjoy the full benefits of the progress made at the end of the last century. For many institutions, this will involve a fundamental re-think of the way in which information, and the systems that process it, are protected. In this context, managing information security-related risk means understanding the risks and responding to them in an appropriate way. This is a fundamentally different approach to systematically adopting 'best practice' solutions and involves assessing risk as it affects a particular business concern. Such an approach should enable organisations to take risk in a controlled manner, which is an essential part of responding to market opportunities.

In this article, some of the more fundamental issues in modern information security are presented and discussed in an attempt to provide an idea of where the problems lie. The remainder of the article aims to show how the intelligent use of established management practices can go a long way to resolving many

of these issues. The essential point however is that there is no single solution to these problems. Individual organisations have their own particular needs and culture and should therefore seek to establish a risk profile that is in line with their own business strategy. This is a statement that sounds obvious but is extremely difficult to achieve in practice – nevertheless, those companies that do achieve this will at least be masters of their own destiny.

Important issues in modern commercial environments

In order to illustrate the kind of challenges that face modern information security departments, a number of issues, illustrative of the kind of problems encountered in modern commercial environments, are discussed in the following paragraphs. For the purposes of this document, these issues can be grouped into one of the following four categories:

- Conceptual issues.
- Business-related issues.
- Technical issues.
- Operational issues.

Conceptual issues are in many ways the most difficult issues to resolve, as they are rooted in the way we perceive security. Apparently simple concepts, such as trust and privacy, become more complex in distributed environments. Consider the notion of trust for example. After a little reflection, most people would agree that trust is not a binary thing. On the contrary, we tend to trust people within a particular context and there are limits to this trust. We might trust a doctor to make decisions about our health, but perhaps not to invest money on our behalf. Continuing with the example of the doctor, some people may trust a more specialised colleague based on his/her recommendation, whilst others may seek a second opinion in this case. This illustrates nicely the notion of transitivity – can trust be passed on to a third party? Finally, it is evident that there is a risk associated with every trust relationship and this risk describes the consequences of a potential breach of the trust. Not surprisingly, these kinds of issues are not easy to quantify [4]. Electronic commerce however involves the establishment of such relationships and it will become increasingly important to correctly understand the basis upon which the trust is established.

Carrying out business across geographical boundaries is nothing new, but the extent to which this is now happening and the pace in which agreements are made and carried out certainly is. In general, the evolution of technology is coping well with new demands placed on it by the increasing pace of business. Other areas are having more difficulties. The rate at which new legislation is adopted for example is far slower than that at which business practices are evolving. In addition, agreeing appropriate legislation is greatly complicated by the different approaches to legislation adopted by different countries. Enterprises that operate in an international environment will experience these problems in several areas, including data protection, privacy and the use of cryptography.

Arguably the most important technical issue is that of complexity. The high level of complexity associated with many modern IT infrastructures often means that most users do not understand how it works. In fact, more often than not, even the experts only understand a part of the infrastructure and very few people indeed appreciate how all the component parts of an enterprise's architecture work together to achieve business goals. This is a major issue for security professionals, as it is difficult to secure something that one doesn't understand.

An example of how complexity has increased in recent years is provided by the move from the single-platform approach to computing to highly-distributed, heterogeneous, computing environments. As a result of this change, sensitive data is likely to be spread across a number of platforms. In addition, the same data might be stored in several different locations, leading to all the problems associated with redundancy (such as ensuring that the data is updated in a consistent manner). Quite often, the technologies that are used to achieve this form of distributed processing aim to render this process

invisible to the end user, on the basis that this makes their life easier. The implication for information security is obvious. Logically, moving to a highly distributed architecture should result in a shift of focus from platform-based security to an approach that takes sufficient account of end-to-end security issues. Unfortunately, this change of focus is often overlooked.

Yet another issue closely related to technology is that of visibility. Internet connectivity has resulted in an increased level of visibility for most connected enterprises. This increased visibility not only allows potential wrong-doers to gather information about a target and launch attacks, but can also lead to enterprises becoming a target *precisely because* they are so visible. In particular, the web sites of large enterprises and institutions are often defaced in order to pass political messages.

Operational issues arise out of the way in which enterprises react to this changing environment. Many enterprises are still relying on a control framework that was designed to secure a much simpler environment and which is now based on assumptions that no longer hold. In particular, control mechanisms and procedures established for single platforms do not necessary scale well to large, multi-platform environments. Pro-active log analysis for example might be perfectly feasible for a group of 10 local UNIX systems, but an entirely different approach is needed to cope with a thousand platforms in ten different countries.

Many of the operational issues that are typical of today's environments are essentially due to the fact that everything is happening faster these days. Looking at the way in which the threat is evolving, it is clear that the delay between the publication of vulnerabilities and the attacks that exploit them is rapidly decreasing. This ability of attackers to successfully exploit the window of risk between the discovery of a problem and its resolution is worrying and is forcing companies to put temporary defences in place before software suppliers provide the appropriate patches or pattern files. Enterprises that have incorporated the idea of 'defence in depth' into their security architecture will be in a better position to respond to these attacks.

Another area in which the need for faster response times is manifesting itself is related to the way software is produced. The need to shorten the time to market in order to remain competitive may result in shorter testing cycles and lead to the appearance of more security-related vulnerabilities. Within the enterprise, information security departments that cannot adapt their methods to accommodate the timescales required by the business will almost certainly be bypassed.

Basic principles

When we combine the impact of the trends and issues discussed above with the fact that most enterprises are being forced to cut costs in order to remain competitive the true magnitude of the problem becomes apparent. Simply put, information security managers have to secure more complex environments, faster and using less resources.

In order to achieve this, it will be necessary to have a clear idea of the principles underlying the overall approach to securing information. For the purposes of this document, the key ideas underlying a successful approach are as follows:

- *The approach should ensure that the level of information security-related risk accepted by the enterprise is in line with business expectations.*

  This involves ensuring that business managers are fully aware of the risks associated with different business alternatives and that any decision to accept or reject risk is taken with this in mind. Note that the requirement does not reference any external standard or best practice. It is quite acceptable to take risk as long as this is done in a controlled manner.

- *Legal and regulatory requirements must be met and it must be possible to demonstrate this fact.*

Even if enterprises are compliant with legal and regulatory restrictions, an inability to demonstrate this may lead to significant additional costs as a result of negative audits.

- *It should be possible at all times to react quickly to business requirements, whilst still continually improving the overall control framework. In other words, the approach should allow for both tactical work and strategic work.*

  Very few organisations have the level of maturity required to satisfy all business requirements using the existing control framework. The vast majority of organisations will therefore need to pursue both tactical and strategic objectives to make the most of business opportunity.

- *Compromise is essential, but it has to be done in the right way. Fast risk analysis techniques should be used to compare alternative actions on the basis of risk.*

  Most security practitioners accept the fact that security is not perfect, but some might find it difficult to accept solutions that are not in line with market standards. The ability to compromise is important in this area, but it is equally important that compromise be achieved in the right way. Fast risk analysis is a useful tool for making management aware of the risks they are taking. If management are prepared to sign off the risk and there is no legal or regulatory issue at stake, this is OK.

There are of course many other principles that could have been cited in this section. However, a deliberate attempt has been made to concentrate on the most fundamental principles; those related to managing the risk. Once these principles have been established, it is possible to define an approach.

A pro-active approach

Information security managers that are convinced of the need to change an existing approach to information security are often faced with an interesting dilemma - notably that this very approach does not allow them to influence opinion where it matters; at the top. Under these conditions, any attempt to introduce change needs to be carefully planned, taking account of the personalities involved and their expectations. This is a key point - analytical documents do not in themselves initiate change, whereas correctly managing relationships within the enterprise does.

For this purpose, we divide the overall plan to re-orient the approach into two distinct phases. The high-level objectives of the first phase, which we shall refer to as the consolidation phase, are to establish credibility, to build up a network of contacts, to identify where changes should be introduced and to wind down any activities that are unlikely to be unprofitable in the long-term. The major deliverable of the consolidation period is the information security strategy. In order to produce a realistic strategy, it will be necessary at an early stage to assess the level of maturity of the current approach, as this will determine how much effort is likely to be spent on tactical initiatives and how much is available for strategic initiatives. In general, less mature organisations will need to foresee more tactical activity, whereas mature organisations will be able to devote more time to strategic initiatives (see figure 1).

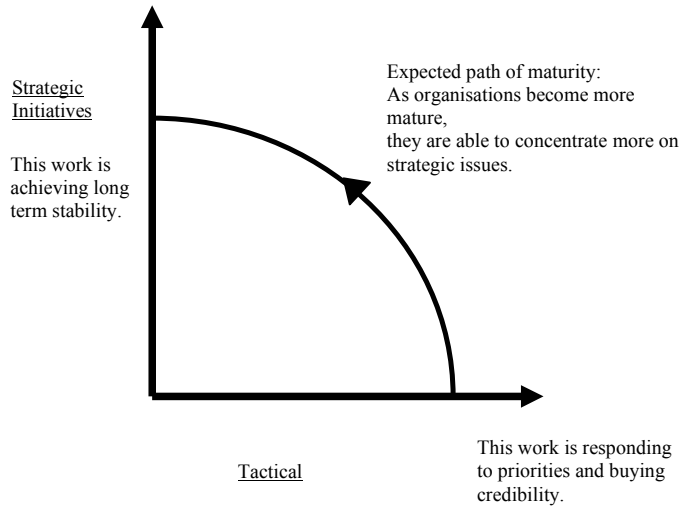

Figure 1

The detailed objectives of the consolidation phase are discussed in the following section.

At the end of the consolidation period, the information security approach should be driven by a series of strategic planning cycles. A complete planning cycle should ideally span a period of about three to five years. The strategic planning cycle encompasses four key steps, which can be thought of as essentially sequential, but which in reality overlap to some extent. The steps are, not surprisingly, the definition of a strategy (which doesn't need to be done for the first cycle as it is done during the consolidation period), the production of a strategic plan, execution of the plan and monitoring and improvement. The strategic planning cycle is discussed in more detail below.

The consolidation period

The consolidation phase can take anything from six months to a year, but it is preferable to keep this phase short wherever possible. Typical detailed objectives of the consolidation period are as follows:

- To identify major stakeholders and ensure their buy-in to a revised approach.
- To understand the strengths and weaknesses of the current approach.
- To classify issues into short-term, medium-term and long-term concerns.
- To provide temporary or permanent solutions to short-term issues and cancelling any ongoing activities not likely to be in-line with the future strategy.
- To identify and take advantage of any 'quick wins' that can be realised before the strategy document is completed and agreed.
- To implement initial management control mechanisms.
- To define the strategy for the next strategic planning cycle.

The first step is critical and is designed to ensure that all the relevant decision makers are identified and involved in the security process. A stakeholder in the information security approach is someone who will be affected by the quality of the result and who therefore has a vested interest to protect. In some senses, all staff are therefore stakeholders in the approach. However, the idea here is to target the decision makers and to ensure that the latter involve their staff. A good technique for identifying stakeholders is to gather and use information on how decisions are made, rather than identifying participants based on more theoretical notions, such as information ownership (this type of exercise can sensibly be achieved

later). A lot of useful information can be gleaned here by paying attention to the composition of steering committees, user groups and similar bodies.

The strengths and weaknesses of the current approach are key inputs into the information security strategy and the task of understanding them can be begun before all the stakeholders have been identified, as there will presumably be documentation (such as past audit reports) that needs to be analysed as part of this process. Nevertheless, staff members themselves are likely to provide the most useful information in this regard. It is therefore important to approach stakeholders, once they have been identified, with an eye to listening rather than talking at this stage. In order to get the most out of these meetings, they should be well prepared in advance and the people being interviewed should know what is expected of them. The details of this preparation are largely a matter of personal style, but should include at least some background information, a statement of the objectives and an agenda.

The issues that arise out of the discussions with stakeholders and analysis of the current approach can be classified into those that can be resolved relatively quickly and those that require a more long-term approach. The overall aim will be to resolve the former within the consolidation period and to incorporate the resolution of the latter into the information security strategy. In reality, issues will be ranked according to several criteria including the degree of associated risk, the complexity of the rectification exercise and the extent to which the issue and likely solution is acceptable to the user community. This will then be used as a basis for detailed planning.

The analysis of the current approach will often reveal opportunities to make improvements at little cost. Although the improvements might be small, their implementation does provide positive feedback to other staff and therefore helps build credibility. If it is not already in place, the introduction of fast risk analysis techniques falls into this category. A simple, pragmatic tool for analysing information security-related risk and identifying appropriate mitigation actions is an extremely powerful tool and can greatly assist the decision making process. Another advantage of introducing a viable approach to handling risk is that it removes the urgency of creating a revised information security policy. This is very helpful, as creating workable policies generally requires a lot of time and effort. Other areas in which quick improvements might be possible include the introduction of simple statistics and regular reporting and establishing a schedule of co-ordination meetings within the information security group.

Whilst all the above tasks are important, the major objective of the consolidation period is to define the information security strategy for the next strategic planning cycle. The strategy itself will likely be based on several inputs, including:

- The strengths and weaknesses associated with the current situation.
- Requirements associated with the business strategy
- Legal and regulatory requirements.
- Requirements due to external trends.

The final strategy is a coherent, high-level description of the strategic objectives and how they will be achieved. Typically, the strategy will provide a prioritisation of major initiatives and an idea of how the objectives will be accomplished as a function of time. However, the strategy will not contain any detailed planning as this is likely to change as the different business priorities change to reflect the way markets are evolving.

The strategic planning cycle

In a nutshell, the goal of every strategic planning period is to ensure that the approach to information security is (and remains) integrated into the core processes of the organisation in such a way that decisions are made by the right people at the right time with the right results.

The approach described in this document is based on the production and maintenance of four core deliverables:

- The information security strategy.
- Policy documents and supporting standards.
- The IT security architecture.
- User awareness and training material.

The first of these deliverables, the information security strategy, has been briefly described above, due to the fact that the first such strategy is typically produced as part of the consolidation period. The information security strategy is the roadmap for the foreseeable future and outlines how the organisation intends to progress along the path of maturity illustrated in figure 1. In particular, the information security strategy explains how the other three deliverables will evolve over time. The second two items in the list above are often collectively referred to as the control framework, whilst the last item is concerned with making users aware of the framework and how to use it to maximum advantage.

The control framework consists of all the policy statements, standards, procedures, working documents and technical measures put in place to secure day-to-day operations. The control framework may be thought of as the slow moving side of the information security process and risk management as the dynamic side of things. This framework changes slowly as a result of strategic initiatives and the extent to which it is capable of successfully responding to the day-to-day needs of the organisation is a good measure of the organisation's maturity. Risk management is the primary tool for verifying the framework in a particular context and for indicating where modifications and/or tactical solutions are necessary. As organisations become more mature, it is expected that the control framework will be driven more by risk assessment than by policy, reflecting the ability of the organisation to quickly react to changes in the business environment. These ideas are illustrated by figure 2.

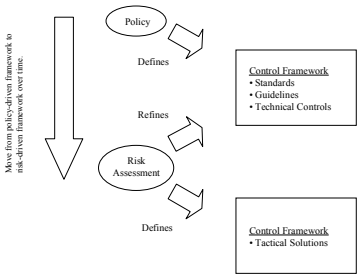

Figure 2

Policies and standards provide a framework for information security by defining rules and guidelines for handling everyday situations. Policy statements are used to define high-level requirements, sufficiently generic to be applicable in a variety of circumstances. Standards and procedures on the other hand are used to translate these high level requirements into implementation details. By interpreting policy within a defined operational context, standards and procedures provide an approximation to the best response to any particular problem. One of the characteristics of well-trained staff is that they are capable of

recognising when a standard procedure is failing to mitigate risk correctly and are able to react accordingly.

Effective and efficient procedures are one of the cornerstones of a mature control framework, but it does not usually make sense to develop such procedures without taking due account of the technology that will support them (similarly, when designing technical solutions it is important to realise how existing procedures will be impacted). The technical tools used to secure the day-to-day environment are therefore an integral part of the control framework. One way to ensure that procedures and technical solutions are closely aligned is to define and implement an IT security architecture. Note that in many cases this does not necessarily involve a lot of additional expenditure, but is more an exercise to make better use of the tools already acquired.

A well designed security architecture brings many advantages to the organisation, including:

- Reduced complexity through standardisation.
- The possibility to improve end-to-end security.
- The possibility to protect platforms that are vulnerable (but which cannot be further secured for one reason or another) by using compensating controls.
- Decreased time to market for new applications.

Developing a security architecture is not easy however and the result should reflect the concerns of the organisation and the risk profile it has chosen to adopt. One way to achieve this is to produce a simple model of the current environment and to conduct a risk analysis against this model. By considering risks across the infrastructure, it should be possible to derive a set of logical components that implement a suitable balance between platform-specific security and 'architectural security'. The idea is that security services provided by the architecture will be provided in a normalised way to all future applications, thereby avoiding duplication of effort and all the additional complexity that this often brings with it.

Last, but certainly not least, the strategy should address the issue of awareness and security-related learning, even if the approach is to maintain what has already been achieved. The fact that many organisations are not giving this subject the attention it deserves is illustrated by a number of recent surveys in the area of information security. Ernst & Young's 2003 Global Information Security Survey for instance, observes that only 29% of organisations surveyed list employee awareness and training as a top area of information security spending [5]. Similarly, the information security breaches survey 2002 [6], sponsored by the Department of Trade and Industry in the UK, reports that only 28% of UK businesses make staff aware of information security related duties on joining or as part of the induction process. Furthermore, according to this study, 13% of UK businesses have no procedures at all for educating staff on their responsibilities in this area.

The correct response to this problem starts with a recognition of the fact that security awareness, although important, is not sufficient in itself to ensure that staff have the knowledge required to react correctly in the face of an incident. Basic awareness training should be supplemented by more specialised training directly related to the function of the employee. This will almost certainly require a way of working together with business lines where both parties are learning. In addition, there are many other informal communications channels within most organisations that can be put to use to train staff. Indeed, every point of contact between the information security department and the user community provides an opportunity to pass a message. Viewed in this way, user awareness and security training is an ongoing activity that is an integral part of day-to-day business, rather than something that is achieved via a series of formal presentations once a year.

Conclusions

Recent advances made in the area of network technology and the subsequent success of the Internet as a medium for conducting business have resulted in a new business model. This new model has resulted in a number of new challenges in the area of information security which, although largely understood, are only partially resolved. As a result, information security-related risk has been growing rapidly in the last few years and companies will need to take a more proactive stance to managing this risk in order to continue to enjoy the benefits that technological advances have made possible.

The issues which confront the present-day security manager are varied in nature. In some cases, it is the concepts upon which our understanding of security is based, that are being put into question. The notions of trust and privacy were cited as examples of this type of problem. Business-related issues on the other hand are often easy to understand, but difficult to resolve. In particular, providing a global legislative framework that is capable of supporting global electronic commerce is likely to be a long and slow process and is complicated by different approaches to legislation at the national level. Many of the technical issues are related to the increase in complexity that characterise many modern IT environments. This increase in complexity often results in an insufficient understanding of how the architecture as a whole functions and this is a major obstacle to implementing appropriate security measures. Finally, operational issues reflect the problems that enterprises are experiencing in adapting to changing demands. This is particularly true where the time to respond is concerned.

Managing information security in such an environment requires a clear idea of the principles that the approach will have to respect. The most fundamental principles are related to the way in which information security-related risk should be handled, as this is the whole purpose of Information security.

This article has described a two phased approach to re-engineering the way in which information security is managed. The major objectives of the initial phase are to establish credibility, to build up a network of contacts, to identify where changes need to be introduced and to wind down any activities that do not make sense from a long-term perspective. The second phase is repeated every three to five years and essentially involves defining, implementing and monitoring a revised strategy.

The information security strategy, the policy and standards, the IT security architecture and user awareness and training material are the important deliverables of the strategic planning cycle. The strategy is to be seen as the high-level roadmap for the current period and this document outlines how the remaining deliverables will evolve. The control framework consists of all policy statements, standards, procedures and technical measures that are used to secure operations. As enterprises become more mature, they improve the effectiveness and efficiency of the control framework. Risk analysis techniques are used to discover how well the framework performs in a particular context and indicate where supplementary, tactical measures are need to satisfy short-term requirements.

Procedures and technical solutions are best viewed as complementary aspects of any approach to mitigate risk. Implementing one without taking account of the impact on the other is likely to result in incoherencies or, at best, inefficiencies. The concept of a security architecture can be used to ensure that both achieve an appropriate response to the perceived threat environment.

Finally, it is important to plan user awareness and training from a long-term perspective. This will typically involve far more than the traditional security awareness campaign and should be seen as a series of initiatives (both formal and informal) that aim to introduce the notion of security risk management into the culture of the enterprise.

References

[1] “CERT/CC Statistics 1988-2003”, http://www.cert.org/stats/cert_stats.html, Aug 2003.

[2] "2001 CSI/FBI Computer Crime and Security Survey", Computer Security Issues & Trends, Vol. 7, No. 1, 2001, pp 1-18.

[3] "2002 CSI/FBI Computer Crime and Security Survey", Computer Security Issues & Trends, Vol. 8, No. 1, 2001, pp 1-22.

[4] S. Purser, "A Simple Graphical Tool For Modelling Trust", Computers & Security, Vol. 20, No. 6, pp. 479-484, 2001.

[5] "Global Information Security Survey 2003", http://www.ey.com/global/download.nsf/International/TSRS_-_Global_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf, Sept 2003.

[6] "Information Security Breaches Survey 2002", http://www.pwcglobal.com/Extweb/ncsurvres.nsf/docid/845A49566045759E80256B9D003A4773, Sept 2003.