

A Proactive Approach to IT Security Management

by: Steve Purser, 02/28/2005

<http://www.securitydocs.com/library/3067>

Note : This paper has been reformatted and republished from our archives.

1.Introduction

In order to remain competitive in mature markets, companies are having to respond quickly to changes in the market place. To respond appropriately, organisations often have to change their own core processes and infrastructure. Time to market for new products is a critical success factor and traditional development time-scales are being further and further compressed to meet the demands of the customer. In parallel, enterprises are being forced to cut their cost base in order to satisfy shareholders and staff are often reassigned from control functions to functions which are directly associated with generating revenue. The net result is that modern organisations are under increasing pressure to produce results faster and at lower cost.

The traditional approach to managing IT security does not perform well in these conditions as the techniques it relies on assume a level of stability, which is rarely present in today's organisations. As an example, security policy documents are usually written to cover a period of several years. This is because updating such documents, which usually requires approval by executive management, can be an arduous process. The rate at which modern organisations undergo re-organisations or participate in corporate re-structuring activities, such as mergers and acquisitions, often puts this approach into question.

The IT security manager in modern organisations is therefore faced with a fundamental dilemma. If he/she does not react to change quickly enough, it is probable that the security process will be bypassed in order to meet business deadlines. Conversely, acting faster than the time-scales the processes are designed to handle may well result in additional risk through error.

The objective of this paper is to present an approach to managing IT security, which is more closely aligned with the requirements of today's business environment. The central idea underpinning this approach is the recognition of the fact that policy statements nearly always need to be interpreted in the light of current opportunities and constraints in order to be meaningful. In moving away from an approach, which is strictly policy-driven, to an approach, which interprets policy in the light of a risk assessment, the organisation has the possibility to accept the degree of risk appropriate to the current market conditions.

In order to take advantage of this flexibility, the IT security strategy and processes themselves must be designed to be flexible and scalable. Adopting an architectural approach, based on an end-to-end view of security, provides an appropriate starting point for such a design as it promotes economies of scale and allows the organisation to make more efficient use of compensating controls than that offered by a system-specific approach.

2.Learning from current processes

2.1 Analyzing efficiency and effectiveness

The goal of implementing a new approach to IT security management is to solve the problems associated with the current approach. Hence, a sensible first step in defining a new approach is to analyse, understand and document the failings of the current approach. To accomplish this, we need to look at both the effectiveness (are we doing the right things?) and the efficiency (are we doing things right?) of the processes we have deployed.

Whilst it is probably true to say that many organisations are experiencing similar, if not identical, problems in some areas (such as the difficulty associated with managing highly granular access rights across different technical platforms), other problems will be specific to particular organisations. The results of the exercise are therefore expected to be organisation-specific.

Useful questions to ask in analysing the effectiveness of current processes include:

- Is the underlying control objective clearly defined?
- Does this control objective address the risk we are trying to manage?
- Is the control objective necessary (i.e. is the risk satisfactorily addressed elsewhere)?
- Is the control objective realistic?

Useful questions to ask in analysing the efficiency of current processes include:

- Is the current process sufficiently scalable?
- Does this process have an unreasonable dependency on specific skill-sets?
- If so, can it be de-skilled?
- Can the current process be executed quickly enough to meet the requested deadlines?

2.2 Examples

The following examples have been chosen to illustrate some of the more frequently encountered problems.

Access control

Problems associated with the access control process include:

- The underlying control objective is usually interpreted as applying to individual systems, rather than to the architecture as a whole. As a result, it is difficult to verify that the access control schema is coherent across multiple applications (so that a user is not denied read access to certain information in one application and granted such access in another).
- In many cases, the control objective is too ambitious – maintaining highly granular access rights in a highly distributed system is an extremely complex and time-consuming activity.
- There is often an unrealistic dependency on skill-sets - representation of access rights is difficult to understand for non-technical staff (and in particular, for those who approve and verify access rights).
- Distributed architectures provide facilities for retrieving data from a variety of sources and presenting it to the user as a single set (e.g. SQL queries). In this type of environment, organisations using a data-centric approach may find it difficult to map access rights to specific groups of data.
- There is usually no consolidated view of access rights covering all platforms. This strongly limits the scalability of the approach.
- An inappropriate workflow process may result in unacceptable delays for the end user.

Security monitoring and log analysis

Problems associated with the security monitoring and log analysis process include:

- The control objective is often interpreted on a system-by-system basis and is therefore too ambitious (as it implies that certain logs should be analysed on every system, which is usually not economically feasible for large infrastructures).
- Where the system-by-system approach is used, the opportunity to use compensating controls is greatly reduced.
- There is an issue with skill-sets. Frequently, logs can only be interpreted by skilled engineers and engineers do not like analysing logs. This leads to boredom and errors.
- This is clearly not scalable to large environments.

Vulnerability detection and management

Problems associated with the vulnerability detection and management process include:

- Systems are scanned against pre-defined baselines. However, baselines are not always designed to reflect real-risk and are often over-ambitious. This can result in voluminous reports, which are difficult to understand, and prevent the definition of an appropriate action plan.
- Detecting vulnerabilities is important, but does not add a lot of value if there is not an action plan for correcting them.

As such action plans often necessitate involving suppliers of third-party software, it is essential to have a structured approach.

- There is a high dependency on skill-sets.
- Use of publicly available software may not be appropriate for medium and large organisations as such software is often not designed to support a highly distributed architecture – leading to rollout and maintenance issues.