



Can IT security give a return on investment?

Graham Titterington

December 2006



Can IT security give a return on investment?

Security vendors have been fighting an uphill battle to get business leaders to spend on their services. Several of them have produced a 'return on investment' tool to help their salesforce win over sceptical customers, but the approach has lacked credibility. The ISO 17799 standard advocates a security planning approach based on risk management principles. It has been in existence for many years, but it has only recently started to win influence in the market. Now several vendors are presenting their offerings in a risk management perspective. This change is welcome as it provides a more realistic view of the role of security and is more prescriptive in suggesting how security can be improved within resource constraints. Graham Titterington examines the Symantec approach to using risk as a planning tool, as this vendor is leading in this aspect.

Why not use 'return on investment'?

The usual definition of 'return on investment (ROI)' is the ratio of the profit resulting from an investment to the cost of the investment. Security is primarily a form of insurance where the 'return' on the investment is in the avoidance of 'cost' that would probably be incurred if the expenditure was not sustained. This of course involves a hypothetical calculation. This is the same with all forms of insurance. The ROI approach is not appropriate for this kind of decision making.

There are some aspects of information security that can be justified on an ROI basis because they render operational savings or deliver other operational benefits, such as:

- virtual private networks, which can replace private leased lines
- automated user provisioning, that removes blocks to user productivity and saves administrative effort
- technology that enables new ways of working, such as mobility or web services.

However, these are the exceptions. In general, the business decision relating to information security spending should be made on the basis of what level of risk is acceptable, and what is the most efficient way of achieving the necessary risk mitigation.



What are the risks?

Risk analysis is about much more than identifying hazards. Every organisation is surrounded by a host of threats and issues needing attention. It is important to consider all kinds of shortcomings, and not just malicious attacks. For example, performance problems, inadequate capacity, oversights, accidents and mechanical breakdowns may threaten assets or the smooth operation of the business. On the other hand, a threat that is not relevant to the configuration or assets of the organisation can clearly be ignored. Organisations already have many defences against a wide range of threats. A threat that would be blocked by the existing defences need not be considered further. Having identified the range of threats that are potentially damaging, it is necessary to determine what impact they might have so that responses can be appropriate and prioritised.

Therefore, risk management is about analysing the interdependencies between:

- threats and issues
- vulnerabilities and weaknesses
- business and operational impact.

Why is security so hard to sell?

The security planning process spreads across different functions within an organisation. If we restrict our attention to the risks relating to information systems we still span two silos: the 'business' and the 'IT department'. These groups find it hard to communicate – they use different vocabularies, and communication between them suffers a 'lost in translation' problem. One of the aims of the risk management approach is to interpret between these different views.

Symantec's INFORM approach

INFORM allows users to benchmark their environment compared with industry standards, using third party research, information collected by Symantec from other users of this tool, and the ISO 17799, ITIL and COBIT standards.

INFORM is a 'facilitated service', not a product. It has two main views: 'security' and 'operational efficiency'. It is based on the CMMI model and its levels of maturity for corporate processes. An organisation is evaluated in several process areas and the results are entered into the model. Default values and default formulae are built into the model to enable models to be built quickly, but users can override these defaults if they



think the organisation's profile is different from that implied by the default settings.

It prioritises areas for attention to get maximum risk impact reduction for any given budget. It provides a framework for comparison with comparable organisations and for discussions about the way forward. It compares the organisation's current practices with ISO 17799 good practice in the security area, and ITIL or COBIT best practice in the operational efficiency area. It does not promote any specific tools, but suggests generic areas for attention – including ones not covered by Symantec, such as access management.

INFORM is designed to be used by Symantec consultants, although clients can refine models that consultants have built and experiment with varying the parameters of the model. The major modules are web-enabled, but not available for public access.



Client re-use disclaimer

- This is a verbatim reproduction of independent material that has previously been published by Ovum within the last 6 months
- Ovum operates under an Independence Charter. For full details please see www.ovum.com/about/charter.asp
- Neither Ovum nor the analysts were paid by the client to write any part of the material
- Ovum may have been paid by the client for the right to re-use the material
- Ovum may have a deal with the client to supply research or consultancy. However, no other relationship exists between the 2 companies (e.g. shareholdings, loans, non-executive directorships etc)
- Ovum does not endorse companies or their products
- While we take every care to ensure the accuracy of the information contained in this material, the facts estimates and opinions stated are based on information and sources which, while we believe them to be reliable, are not guaranteed. In particular, it should not be relied upon as the sole source of reference in relation to the subject matter. No liability can be accepted by Ovum Limited, its directors or employees for any loss occasioned to any person or entity acting or failing to act as a result of anything contained in or omitted from the content of this material, or our conclusions as stated
- This material is the copyright of Ovum Europe Ltd.