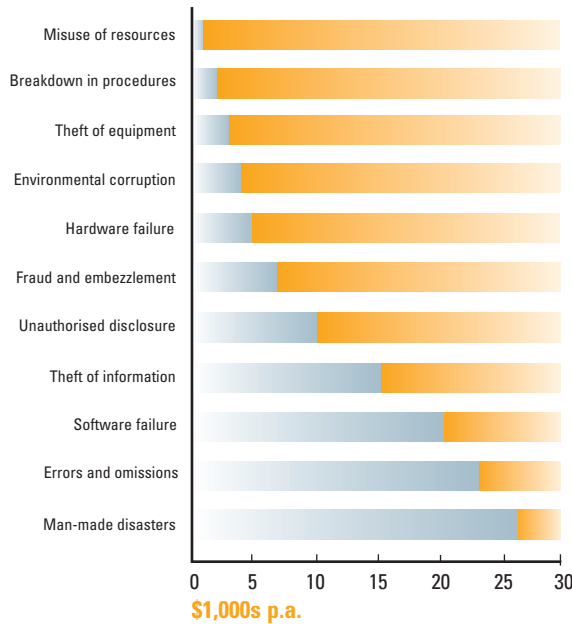


# EFFECTIVE RISK ANALYSIS: WHAT YOU NEED TO KNOW

**Kevin J. Fitzgerald provides some answers for vulnerable management**

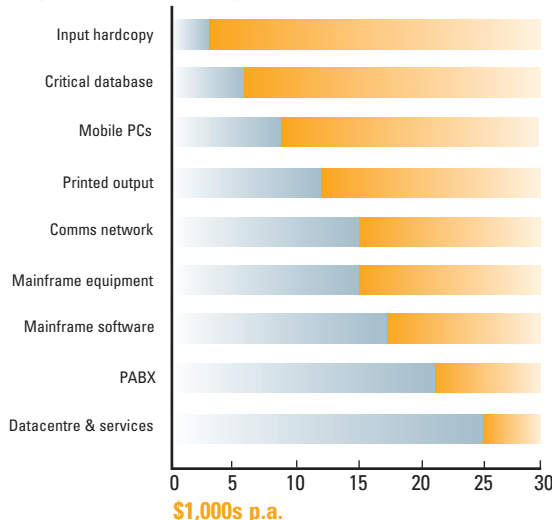
Imagine the possibility of knowing what your organisation's risk profiles look like

### THREAT PROFILE AS SAMPLED FROM ACTUAL RISK ANALYSIS PROJECT



### VULNERABILITY PROFILE

A sample illustrating what risk workshops can reveal about an organisation's vulnerability



**R**isk analysis is a means by which management can analyse their organisation's susceptibility to security threats. This analysis will guide budget and implementation issues to ensure the greatest protection at the best price, but few organisations have bothered to clarify their security position. The majority favour living in a fool's paradise, preferring ignorance instead of investing adequately in security.

In the past, management has been able to get away with a degree of ignorance about security but this is going to be increasingly difficult because of:

- 1 Increased security requirements from corporate regulators;
- 2 The integration and open access paradigms like e-business and the Internet into core business practices; and
- 3 The new standards for security now regarded as 'mandatory' by auditors (Standards Australia: AS/NZS ISO/IEC 17799).

The combination of these three factors, let alone other pressures such as corporate liabilities and responsibilities, privacy legislation and basic productivity issues, mean management cannot continue to ignore security issues (see graph, above left).

### Wouldn't having access to such profiles help you to:

- Prioritise your security effort?
- Confidently choose to tolerate lower-ranking threats?
- Become aware of your organisation's most vulnerable assets?
- Create the arguments necessary to win a security budget?
- Become proactive about security rather than taking the usual beating from the auditors?
- Reduce the number of surprise incidents?
- Give management and staff an understanding of why security should be looked at positively rather than negatively?

The AS/NZS 17799 standard urges that risk analysis be a foundational tool for managing risk in the corporate world.

Is your interest in risk analysis increasing? Well it should be if you are a CEO, CFO, CIO, COO or company director. It might help to know the typical questions executives ask when considering risk analysis. These are some I have encountered in organisations large and small.

### What are the prerequisites for effective risk analysis?

Executive sponsorship. In many organisations security has been considered a 'necessary evil' for so long, it must have strong sponsorship to take it to a new level and to cultivate enterprise-wide acceptance.

Establishing a base-line security effort will be a worthwhile warm-up to the more comprehensive cover the risk analysis will suggest. Creating a security policy and standards manual is a typical starting point. It can provide a formal reference point for all managers and staff. It should signal the beginning of security training and the acceptance of security responsibilities. Again, this is referred to in the Australian standard as a necessary foundation.

### What is the scope of an effective risk analysis?

It is usually focused on the three areas of information security:

- Confidentiality, information and related assets can be classified on a need-to-know basis and treated accordingly.
- Integrity, information and related assets must be complete and accurate.
- Availability, information and related assets must be available to users according to the business's tolerance for being able to operate without the applications or systems.

Risk analysis of information security involves elements of physical security – personnel security as well as information security itself.

However, a risk analysis of the information security environment may well be broadened to cover risks associated with:

- IT practice management. Undisciplined practices can represent major threats. For example, allowing the application of software patches to be delayed is a common costly occurrence.
- Contract terms. Poor contract establishment or operational management often favours the provider, with the user being left with expensive penalties.
- IT-business alignment. The objectives and goals of the IT department and the business may be in conflict.
- Outsourcing versus insourcing. The economics of this choice are worthwhile revisiting from time to time.
- Asset ageing. Old systems can represent sizable risks and must be reviewed.

### What is the difference between quantitative and qualitative risk analysis?

Quantitative risk analysis usually takes an approximation approach and identifies an approximate dollar cost of an event occurring (its impact), as well as the approximate likelihood of its occurrence (probability). ('It's better to be approximately correct than precisely wrong.') For example, embezzlement in the accounts receivable application may be assessed as having an impact of \$50,000 if it did occur, and its probability of occurring as being once every 10 years. This can then be expressed as a \$5,000 risk per annum.

A qualitative approach may rank the impact and likelihood using a scale of one to six, where one is low and six is high. The results can then be multiplied to be expressed as a single figure. In both cases these single figures for threats and assets can be ranked to provide the threat and asset profiles.

Which is better? It depends on the culture of the organisation. Many prefer the result expressed as dollars so it can be related to the cost of the solution. ('Why control a \$5,000 risk with a \$15,000 solution?')

The credibility of these findings, however, strongly depends on the quality of business judgment that is available to make the decisions evaluating the risks associated with each threat.

### Do I only get problem definition or do I get recommended solutions as well?

Your choice. Guidance for security solutions is available from most consultants in this field. Actually selecting and implementing the solution, however, is often left to in-house staff unless they need a systems integrator to complete the security task for them.

### What resources are required?

In large organisations the best results require experienced operators and managers to be involved in a five or six-day workshop. This is the main data collection phase of the exercise and should be followed up by clarification sessions and review sessions as the report gradually takes shape.

The number of staff and managers required ranges from about 12 to 20 people. They will come from a mix of business, audit and information technology managers and staff. An experienced external information security consultant should be employed to give objectivity and to avoid

the politics. He or she will be the program's report writer and will need to speak to a wide variety of management and staff to successfully complete the analysis.

An effective project can take three to four weeks for a risk analysis alone, six to seven weeks with solution guidelines. Depending on your requirements and the size of your organisation, a risk analysis can cost between \$50,000 and \$80,000 if the focus is limited to information security alone. It will cost more if the focus is broadened to include such things as IT practice management or contract terms.

### How can I afford the resources required?

In a typical situation, management will consider a risk analysis project if the company has suffered recent security incidents that indicate serious risk exposure, or if it has received criticism from auditors, suppliers, partners or customers for having security weaknesses.

Rather than take a 'point solution' approach, which addresses single problems as they occur, it is wiser to obtain the warts-and-all diagnosis so that a proactive security group can be established. When management understands the full risk exposure picture, they can make a stand to resolve the most critical issues and schedule solutions for less critical situations later. In this way, security can be managed positively rather than management continually being on the defensive.

### Has the Internet changed the way we think about security?

Many organisations are increasingly exposed to security threats as they embrace the Internet as a major tool in the fight for a competitive edge.

However, the Internet is a double-edged sword. It represents compelling economic advantages on the one hand; on the other it is a system that was never designed to be secure.

How can you afford not to attack the security problem at its roots? Define your risk exposures first, then find the solutions. □

**KEVIN FITZGERALD**  
is an information security consultant with more than 25 years experience designing and executing security solutions for large organisations.