

# The seven deadly sins

**Purging your security misdeeds is just a matter of being systematic, writes Kevin Fitzgerald.**



**T**here are seven reasons why your information security solution may be found wanting.

## 1. You don't give it sufficient budget

Budgetary consideration is given to the obvious problems that must be solved because they cost time or dollars or both. Thus there is widespread implementation of password access systems, firewalls, and backup systems. But dollars are not found in many organisations for issues of a broader and more basic nature, such as information security policies, business continuity plans, and risk analysis projects. For a long time now passwords have been labelled a 'pretend' security solution, particularly where the access needs to get serious. Firewalls without regularly updated patches and reviewed logs are only a cosmetic solution, and backup systems without regular testing are a waste of time. (How often do we see a tape-based backup system still

in place when the system tolerance has shrunk from two days to two hours through the use of online access, often through the Internet?) In these days of cost cutting and staff trimming, exposing the business to a major computer meltdown is false economy.

## 2. You haven't made it enterprise-wide

Information security can no longer be considered an IT department issue. It needs to filter throughout the organisation. Information must be handled as an asset, not just a commodity. Assets must be handled with respect. Information in all its guises — voice, telephone, fax, email, written, printed, white-boarded — must be considered.

All staff must be involved in recognising the information asset. Managers involved with physical security and personnel security have to plan alongside the information security officer — ideally in an integrated manner.

## 3. You haven't got it all covered

Security is often considered as just a confidentiality issue, but it must cover both integrity and availability aspects as well. Integrity refers to the completeness and accuracy of the information. Thus carelessness, errors, and deliberate unauthorised changes (for instance, the creation of fraudulent or embezzlement schemes) need to be covered. Availability refers to the ability to provide continuous information services for core business functions despite electrical, physical or logical problems. Confidentiality, integrity and availability (CIA) are the cornerstones of the information security mission.

## 4. You have never really given yourself a chance to understand the whole problem

Without conducting an information security risk analysis you will not have an informed view of what your organisation's information security priorities should be. When you understand what your full book of risk exposure priorities are, you can build the business case for addressing each exposure. Without this understanding you will inevitably over-spend in some areas (for example, technical intrusion detecting) and under-spend in others (for example, staff selection for sensitive jobs).

## 5. You have concentrated on technical solutions to the exclusion of people solutions as well

Information security exposures most often involve people. Thus by adding people-management techniques to the solution mix, much more effective control can be achieved. Staff selection, employment contracts, job descriptions, performance reviews, career management, and exit interviews can all be studied with information

**'Information security can no longer be considered an IT issue. It needs to filter throughout the organisation.'**

security solutions, penalties and rewards.

## 6. You have taken a short-range view

A quick fix, often executed under pressure, is just that. It cannot be relied upon. Manufacturer-supplied passwords that are never changed (but known to any hacker worth their salt), firewalls with logs that are never reviewed, risk analyses that are never revisited, and business continuity plans that are never maintained are examples of inferior long-term planning.

## 7. You have not taken a structured approach

Information security is based on four elements: risk analyses; policies, standards, and procedures; management accountability; and regular review. With these elements in place, a security profile and its exposures will be fully recognised, and solutions based on widely understood policies. The process will create its own continuous improvement cycle through regular review.

By addressing these seven issues, your organisation will have security solutions that have their own solid business case, and that address people as well as technical solutions. □

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