

GIVE SECURITY MORE ATTENTION

IT environments are at greater risk than ever before. Kevin Fitzgerald says it's time to stop treating security as the poor relation in the IT spend



It is unacceptable, unaffordable and just unwise to let IT security problems occur in business and then try to fix them after a breach has occurred.

Traditionally, management has been reluctant to invest in robust security strategies until it has experienced a serious security breach. Many companies are reliant on baseline controls such as passwords and virus filters for protection because anything more robust is seen as a questionable cost.

Traditionally, expenditure has gone to the glamorous and easier to justify improvements to customer service systems, or that leading-edge system that offers competitive edge. Often security is the poor relation in the IT budget.

The key reason for this is that management has not really understood what their security problems look like and the risks they present.

In many organisations, IT security is a part-time role given to the IT operations

manager who is only able to give minimal time to the job.

Security-conscious organisations have a different attitude and a 'security culture'. But even they fall into the trap of slavishly 'following the security manual'.

Proactive security measures are necessary to guard against modern security challenges such as misuse of the Internet by users, fending off denial of service attacks, and securing corporate notebooks during overseas trips. The auditing fraternity has gained much power in recent times through pinpointing security problems that show many companies rely on measures that are often just cosmetic.

Executives need to realise that older enterprise systems are based on older mainframes – with older applications and operating systems. Unless these have been updated they will have inferior security by today's standards. Network managers must have sufficient time, and tools, to provide adequate secu-

rity measures for all their internal and external network traffic.

The Internet was designed to be open and easy to access. Internet security is weak – and every systems engineer (not to mention hacker) worth his or her salt knows it.

The desktop environment is commonly cheated of its veil of security by users who bypass the controls for ease of operation and get away with it daily.

How can management quickly gain an organisation-wide understanding of their IT security needs?

Effective and comprehensive risk analysis will give a broad view of the risk exposures confronting business applications. In workshopping a risk analysis, experienced operations managers will be able to deliver a clear picture of the organisation's exposures to threats across all IT assets.

Threats to the confidentiality, integrity and availability of information can all be evaluated. When the exposures are ranked, a defensible perspective of IT security issues can be created. Often management sees for the first time where investment must be made.

A threat such as a flood in the computer room from a renovation accident may happen once a decade and be assessed in a risk analysis workshop as costing approximately \$750,000. However, a common error which occurs, say, 1,500 times a day and costs about \$50 to detect and correct may be considered more significant in the rankings.

Vulnerability tests are more focused on the technical aspects of security. Specific tests will reveal the effectiveness of firewalls, weaknesses in legacy systems and the holes in network security. A vulnerability testing program works well within the risk analysis exercise to deepen the probe into the security weaknesses of an organisation.

Together they can arm man-

The Internet was designed to be open and easy to access. Internet security is weak – and every systems engineer (not to mention hacker) worth his or her salt knows it.

agement with the knowledge that will direct their security spending and provide a positive risk management approach to security.

Many of the controls selected by this approach will be managed and used by people. If their attitude is about 'beating the security system', controls will be seen as a limiting factor rather than an enabling factor.

Unfortunately this attitude exists in many organisations today. Thus it is imperative that management takes a deliberate step to change the organisation's view of security.

Role models can be developed by establishing a program which rewards management and staff for displaying 'good security practice'. Induction, job definitions, training, policies, personal assessments and incentive agreements will all work towards changing attitudes towards security.

Organisations that do this will create a corporate IT security culture that will be self-sustaining, will be proactive and will produce measurable improvements in security performance. □

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