

Culture bound

Creating a corporate culture that is vigilant about security can be achieved with carrots and sticks, writes Kevin J. Fitzgerald.



Company directors today are confronted by governance, legal, and auditory pressures to do better in relation to protecting their organisation's information. They have already installed the typical technical security devices — firewalls, password systems, physical locks and barriers, backup systems, and problem reporting systems — but still we see security problems occurring. The business community has never succeeded in avoiding the occasional unwanted surprise that can come from the bowels of a computer network. And research indicates that the majority of security incidents are perpetrated by employees, not by external parties.

What do we need to do?

The solutions currently implemented ignore two essential factors: the need to build management's understanding of information security as a risk management issue, and the effective change of employees' attitudes towards security.

Technology alone will not provide the solution. It requires a mind shift that addresses the social side of management and employee behaviour. This approach involves training, guidance and encouragement. Such an approach could be described as a 'pull' factor where personnel are encouraged to behave in a manner appropriate to the risk exposure identified. Employee behaviour can also be shaped by the presence of counselling, penalties, and punishments. Together with the more technical solutions, these could be labelled as 'push' factors where personnel are forced to behave in a particular way. This latter force, when used alone, often results in the employee attempting to find ways around the controlling device.

It is contended that, when used together, the encouraging 'carrot' and the enforcing 'stick' have a much stronger chance of providing the result we seek.

The culture of the organisation will change as security

improvements are declared from the CEO down. Management and staff will support one another in maintaining the level of security agreed to ensure that the business operates inside its accepted risk limitations. As a result, management will see a positive return from investments in security, which will be a welcome change, encouraging further investments and further strengthening the corporate security culture.

What is a security culture?

It is a set of behaviour patterns that consistently surface on a daily basis, in such things as management style, employee relationships, management-employee communications, personnel policies, resource allocations, pricing and profitability expectations, customer servicing, business system design and implementation, staff training, and security policy development.

It consists of three elements:

- The definition of the security problem as a risk management problem.
- An implemented set of appropriate technical security solutions, together with security policies, standards and procedures to be used every day, reflecting the organisation's risk.
- A personnel policy with practices, which encourage positive computing activities benefiting the organisation as well as the individual.

It is the third of these elements that deserves more attention as it is usually given scant attention in practice today. The personnel policy is at the core of the change management process necessary to achieve the mind shift for real security improvements.

The well-accepted 'social bond' theory from criminology research provides a framework for the development of

'People are naturally inclined to commit crimes unless a strong social control mechanism exists'

social behaviours that will encourage employees to adopt a disciplined approach to security in their day-to-day work practices. This theory assumes that all people are naturally inclined to commit crimes unless a strong social control mechanism or social bond exists. The theory assumes that:

- A person with strong ambition and self-image will shy away from criminal activities — he will lose what he has already established in his reputation.
- A person with a strong teamwork ethic will not be inclined to become involved with criminal activities — he will lose self-esteem and hurt his team members.
- A person who believes that computer abuse is a criminal activity will be less inclined to criminal activities — because it is illegal and he will be punished if discovered.

To make the social behaviour point clearer, the reverse of all of the above cases is also true.

An effective security culture creates healthy attitudes among management and staff. It encourages them to believe that they will be rewarded for achieving their career goals, being a team player, being security vigilant, and being advantageous to their corporation. □

KEVIN FITZGERALD

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