

A well-trained, well-informed workforce is one of the most powerful weapons in an information security manager's arsenal.



There are many reasons why, including:

- People are very good at spotting irregularities; much better than machines.
- A significant proportion of information security incidents occurs through staff not knowing or understanding.
- Well-motivated staff will report (and act upon) trends and incidents that no mechanised process could realistically hope to detect.

The key word is motivation. Without sound motivation, no amount of knowledge or understanding will change staff behaviour. What is needed is appropriate knowledge and understanding accompanied by appropriate action.

Any information security initiative should be accompanied by a parallel education and awareness initiative. How this is done depends on many different factors, including:

- the level of perceived risk
- available budget – often dependent on the level of perceived risk
- the technical infrastructure of the organisation affected
- geographic spread
- corporate culture





The issue of education and awareness has been addressed in a number of ways, some successful and others blatantly not so. Many initiatives fail because they are unstructured. There is a growing trend to treat them as objective-driven projects.

The core result from such initiatives should be a change in behaviour.

For more information on *Achieving best practice in your business*:

- Visit our website at www.dti.gov.uk/bestpractice
- Call us on **0870 150 2500** to order from our range of free best practice publications or visit www.dti.gov.uk/publications
- Contact your local Business Link adviser by visiting the website at www.businesslink.gov.uk or calling **0845 600 9 006**