

# IY5512: Coursework 1:

## Worked solutions

---

1. *Define the notions of a mandatory security policy and a discretionary security policy.*

A **discretionary security policy** is one set by users. In the context of access control, a discretionary policy is one in which decisions about access are made on the basis of settings provided by the **owner** of the object; the identity, **groups** and/or **roles** of the subject; and the nature of the access requested.

A **mandatory security policy** is one imposed by a central authority (e.g. a security policy administrator). In the context of access control, a mandatory policy is one in which decisions about access are made on the basis of the **classification** of objects and the **clearance** of subjects, and on the nature of the access requested.

Typically a mandatory policy is used in addition to a discretionary policy, and access must be granted according to both policies for it to be permitted.

2. *Describe one way of computing the **impact** (loss expectancy) of a threat as a value (in a currency of your choice), where impact combines the seriousness of a threat with the likelihood of it being realised. You may suppose that you have some idea of the cost to your organisation if the threat is realised, and also that you have an estimate for the probability of threat realisation.*

One possibility is to compute the impact (loss expectancy) as the product of the cost of realisation of the threat and the probability that it will arise during a fixed period of time (e.g. a year).

3. *How might a financial estimate for threat impact be used to decide whether or not to implement a countermeasure to the threat? What shortcomings are there in taking a purely numerical approach to risk management?*

The cost of implementing the countermeasure (for a year say), can be compared with the annualised loss expectancy. If the loss expectancy is greater than the cost of deploying the countermeasure, then it is worth deploying the countermeasure.

One disadvantage of such an approach is that the cost of a threat cannot always be easily quantified. For example, whilst the direct cost of a fraud might be quantifiable, loss of reputation to the organisation subject to the fraud is not so easy to quantify. Thus the comparison approach may be made on the basis of incomplete data.

4. *Accountability requires every action to be assignable to a single individual. Privacy requires that some actions can be made in an anonymity-preserving way. Are these notions irreconcilable?*

This question has no simple answer. It has been the subject of widespread debate for some years. Ultimately, some kind of compromise has to be made between civil rights and the need for accountability.

The situation is complicated by commercial interests. That is, there is also a tension between commercial interests wishing to learn about user behaviour on the Internet (e.g. for targeted advertising) and the desire of users for privacy. This is also a hard problem, since free services that almost all of use, e.g. Google searching, are to some extent funded by focussed advertising based on retained personal information. That is, the price of free stuff is typically some loss of individual privacy.