



Vulnerability

The following risks give some idea of the general vulnerabilities that we, as individuals, and the Company as an organisation, are subject to:

- deliberate or accidental damage to property or equipment;
- unauthorised removal of personal property, company property or information;
- actions of terrorist or antagonist groups in disrupting business.

Information forms a major element of the Company's business and if it falls into the wrong hands this could have far reaching effects on the integrity, confidence in and commercial viability of the Company. All staff must therefore regard all Company information as being sensitive and make sure that they do not disclose it to anybody unless they are certain that the person has a right to it. In case of doubt staff members should refer requests for information to their immediate supervisor.

All staff members should be aware of the type of risks that we might be vulnerable to; for example:

- theft and exploitation of sensitive information and documents. This may be done in order to gain financial advantage, or for other, less obvious reasons;
- loss of documents inside the Company or outside at meetings or when travelling;
- intentional or unintentional disclosure of sensitive information to agencies such as the press or agencies seeking to make profit. Accidental disclosure can take the form of careless talk in places such as lifts, wine bars, trains, etc.;
- careless behaviour or action, such as leaving sensitive information in general areas, leaving discarded copies in waste bins or papers in photocopiers;
- interfering with computer software or data; for example by "hacking" into the Company's systems;
- deliberate destruction of computer programs;
- overhearing conversations in open offices or over telephones;
- allowing visitors or non-authorised staff to enter controlled areas;
- subversion of staff through bribery or blackmail;



- fire and other destructive mechanisms.

It is possible that many small pieces of information can be assembled, much like a jigsaw puzzle, to provide the determined “agent” with a comprehensive and perhaps highly damaging picture with which to operate against or profit from the Company. The disclosure of any information outside the Company must therefore be guarded against.

Assessment guidelines

The magnitude of a risk depends upon the probability of the threat and the impact. Impact in turn depends upon the value of the asset at risk (i.e. how much damage might be done) and its vulnerability (e.g. An office building is very valuable. It could cost millions of pounds to replace. It may be vulnerable to fire, explosion or even earthquake. It is far less likely to be stolen.)

There are three main categories of vulnerability:

- **confidentiality** - the value that comes from an information asset being not generally available outside of the business, which can be impaired if the information is made available to others in an uncontrolled manner;
- **integrity** - which may be considered to be fitness for purpose, an asset is functioning correctly, information is complete, accurate and as up to date as expected;
- **availability** - the need to have an asset available when required by the business;

These vulnerabilities can be further subdivided between accidental and deliberate. In some cases the impact is unaltered (it makes very little difference to the business whether an asset which is needed is destroyed accidentally or deliberately) but it can make a considerable difference to the controls needed to prevent, detect or control the risk.

If the prime vulnerability is because of accidental threats, controls which guard against deliberate threats may not be so important. Care should, however, be taken. If an asset is not protected against deliberate threats, legitimate users may see this as an indication that the asset is not of value and become careless.

Assessing confidentiality requirements

Risk Assessment Guidelines



How much damage to the Company or its business interests could be caused by loss of confidentiality of the information (e.g. information is accidentally or deliberately made known to individuals or the public)?

Low Very little damage - the information is public or of little value to a competitor. Anyone may read the information if they wish.

Medium Some damage - the information could cause some embarrassment if made public. There might be some advantage lost to the Company or a party who entrusted information to the Company if the information were known by competitors. There are laws or contractual agreements requiring reasonable confidentiality measures (e.g. the Data Protection Act) but the information is not highly sensitive.

High Significant damage - the information would be highly embarrassing if made public or there would be significant advantaged lost to the Company, or a party who has entrusted information to the Company, if the information were known by competitors. There are laws or contractual agreements requiring reasonable confidentiality measures and the data is sensitive.

Assessing integrity requirements

How much damage to the Company or its business interests could be caused by an impairment to the integrity of the asset (e.g. equipment which appears to be operating correctly when it isn't, information which appears to be correct when it is inaccurate)?

Low Very little damage - little change of any significant defect going unnoticed, information is treated as indicative or aide memoir.

Medium Some damage - could result in lost business, information is relied upon in making important business decisions.

High Significant damage - visible disruption to the Company, misleading information published, potential to be used for fraud involving significant amounts of money.

Assessing availability requirements

How much damage to the Company or its business interests could be caused by loss of availability of the asset (e.g. equipment breakdown, destruction or theft - individual

Risk Assessment Guidelines



unavailable - information unavailable through equipment failure or lost through destruction of media)?

Low Very little damage - asset is not easily destroyed or damaged, can be easily replaced, has little chance of theft as realisable value is small compared to the effort of removing - business could continue without the asset or there are similar assets that could be used elsewhere in the Company. Information is readily available elsewhere or could be recreated at little costs.

Medium Some damage - asset would have to be replaced at a reasonable cost and reasonably quickly. Business would be significantly less efficient or effective if the asset was not available for more than 1 business day.

High Significant damage - visible disruption to Company business. Bad publicity likely if the asset is not available for more than a few minutes at a key time. Asset is small, valuable and easily disposed of for cash (e.g. computer chips).