Information systems and services

Information requirements differ greatly from one organisation type to another, depending on the nature of the business. But the categories from which this information is available remain similar.

* Internal

* External

* Personal

* Employment

* Financial

* Legal

* Other

For a computerised information system to be useful, it must be capable of organising and presenting information to the context of the business. The following report will compare differences between internal and external information sources relevant to four different organisational types, only one information type will be used per organisation. Examples of its end use will be outlined along with an over view of security requirements which apply to the use and storage of the information collected.

Internal & External Information Sources

As the name implies an internal source of information is information, which is gathered from within an organisation, and an external source from out with the organisation. Examples of internal sources of information are accounting

ledgers, production/sales statistics, staff questionnaires/interviews, training records, internal market research, the list is unquantifiable and what is relevant is dependant on the organisation itself. Examples of external information sources could be information obtained from trade publications, legislation, economic reviews, competitors and market surveys.

Scientific Organisation

Internal

A scientific organisation may collect specific internally generated data about individuals for e. g. a Clinical Trails organisation may collect the following data.

* Reactions to treatment by individuals (Personal)

External

External data used within this sector may be gathered from the following sources.

* Legislative & Legal guidelines for clinical trials

The data stored within a computerised system may be used to generate information/reports, which could indicate whether or not a new treatment or drug will be made available for general use, from both a medical and legal perspective.

Charity / Voluntary Organisation

Internal

A charitable or voluntary organisation may collect various forms of financial data for e. g.

* Details of charitable donations (Financial)

External

External data may be derived from the following sources.

* Legislation and legal documents - such as those outlining guidelines specifically for not for Profit Organisations.

Financial data may be processed within a computerised system and used to plan future activities within the business, like for e. g. whether or not the organisation can afford the financial burden of a new project, or to buy new equipment etc. The legal information would help provide guidelines as to what the money could actually be used for.

Educational Organisation

Internal

An educational organisation e. g. (College), gathers many forms of internal data, like for instance, statistical data on performance e. g.

* Examination pass rates (Statistical)

External

External data within an educational organisation could come from sources such as:

* Other similar institutes (Annual Reports)

The data may be processed within a computerised system and the information generated used for a variety of purposes such as; course type and content evaluation, re-assessment of courses provided e. g. were pass rates poor for a particular course, do the entry standards need to be raised? Or internal market research purposes.

Commercial Organisation

Internal

A commercial organisation like for instance a (Car Production Plant) may gather data related to material and labour usage. For example;

* Job labour and material transactions (Operational)

External

External information may be gathered from various sources. Intermediate sources may also be used e. g. on-line inventory management companies, which provide on-line parts/materials locator services. Other sources include;

* Research and development information provided by other companies and regulatory bodies (Trade Publications)

The data gathered could be used to produce information/reports, which could then be used to forecast future material/labour requirements.

The gathering of information within these organisations basically allows them to;

* Record - evidence and details, in order to;

* Monitor - with a view to improving performance e. g. improving student pass rates;

* Plan - to use what has been recorded and monitored to improve profits through better forecasting and manpower planning.

With the use and storage of information within a computerised system comes certain responsibility.

No longer is the information retained within one secure room which can be locked or at the hands of a few chosen individuals, it is now under threat.

Security Requirements

Computer Misuse

A threat is something that may damage the confidentiality, integrity or availability of a computer system. Although the event causing damage may never occur, the threat exists if there is a possibility that such an event might arise. The value given to the threat is based on the probability of the event occurring e. g. the threat of inaccurate input is high while the threat of fire is usually low. Obvious threats would be threats from system failure, corruption, viruses and outside hackers, all to which of course the organisation must protect itself by the use of appropriate virus protection, firewalls and regular back up procedures.

In an attempt to address some of the above issues The Computer Misuse Act was introduced on 29th August 1990. The main aim was to cover areas for

which existing legislation did not appear to have any legal standing, like hacking and causing malicious damage through computer viruses. Basically it made hacking illegal but is still a shady area where prosecutions are concerned, and is not yet watertight at present.

The organisations above and the data, which they hold represent a great deal of work and accumulated knowledge. If they are not kept safe then they could expect to lose them - replacing them would be an impossible task. It would be equally disastrous if the data were corrupted and therefore unusable, or if any part of the data was revealed to someone who had no right to this information. It is vitally important that the information can be seen only by those who are authorised to see it and can be changed only by those who are authorised to change it. This may be achieved in several ways for e. g.

* By applying passwords/profiles - whereby these would be tailored to the individual and kept confidential.

* Levels of privilege - limiting access to data. For e. g. read only to certain individuals and - read - write - delete to the originator.

The implication of information being tampered with could be disastrous; could you imagine what consequences could arise if the Clinical Trials Organisation did not have adequate security and subsequently had medical results tampered with? Or if the Car Production Plant had its material/labour transactions deleted and was unable to forecast future requirements?

These are just a few of the security issues which must be considered when implementing a computerised information system within an organisation.

Data Protection

The Data Protection Act was introduced in order to protect individuals with regard to the processing of their private data or information. Any organisation or anyone processing personal data must comply with the eight enforceable principles of good practice. They say that data must be:

* Fairly and lawfully processed;

* Processed for limited purposes;

* Adequate, relevant and not excessive;

* Accurate;

* Not kept longer than necessary;

* Processed in accordance with the data subject's rights;

* Secure;

* Not transferred to countries without adequate protection.

This act applies to all users of information systems irrespective of where the data is collected or processed within the UK.

The organisations that tend to be most at risk of breaching the Data Protection Act are those whose business it is to collect and sell information about individuals for marketing purposes or is so large that it is difficult to

keep track of the personal data held. Organisations like the ones outlined should place great emphasis on the act and the obligations it imposes, if personal data is handled as part of a person's job. Failure to comply can mean that an employee is personally liable and may incur a large fine and receive a criminal record.

If individuals are caused damage and distress by breach of the act there are rights to compensation, which can ruin a person's career or indeed bankrupt a company. The act applies to personal data (information that relates to a living person) whether it is held on a computer system or a piece of paper and there are particularly strict rules surrounding certain sensitive data. These include matters relating to health (Clinical Trails Organisation as outlined earlier), sexual life, religious beliefs, political opinions, racial background, trade union membership and criminal offences.

Records must also be kept up-to-date and accurate. To a certain extent an organization is always reliant on individuals to inform them of any changes in their details. However, organizations must review their files regularly to check whether they still need data on specific individuals and then remove that data if not needed.

Copyright

As well as the organisation and the individual, the software manufactures have laws over which they are protected also. This comes in the form of the Copyright Designs and Patent Act. Using pirate software lays the individual and the organisation open to prosecution under the Copyright Act. In addition, the use of non-standard software may cause difficulties with

Systems Management and with communication between PCs and could contribute to system performance degradation. The copying of software for security purposes is generally permitted, provided that the copies are used only if the original version becomes corrupt. The software licensing conditions should be consulted before copying software, to check for any constraints.

Summary

In times where we are becoming more and more reliant on Information Technology it is important that companies learn to use the most relevant sources of information available, in order to monitor and plan future activities. It is also important that information is handled with care and used within certain legal guidelines as outlined above, in order to protect both the organisation and the individuals from criminal liability. Information is now as valuable a resource as money therefore must be treated with the same respect and looked after with adequate security to protect from theft, corruption and misuse. In order to achieve this it is important that the guidelines outlined above are followed and that all individuals employed in the use and storage of data understand that all systems, programs, and data are vital company assets. They also need to know and receive training about the risks and penalties associated with the Data Protection Act and Copyright Infringements, including software piracy.