

Information Risks

► Information risks have long been underestimated and inadequately managed. Generally, companies should be able to control information risks themselves, though specialist assistance may be required for the protection of data networks, etc. It is essential to identify the centrally-held information in a company and what information is key to business success. You should develop secure operations from the start and apply effective security arrangements.

Information is an important factor in production

All companies have information that is critical to their operation, such as customer and production management information, product ideas, marketing plans, etc. There is a **lot of information and it exists in many forms**: personal expertise and experience-based knowledge; agreements; instructions; plans; other paper documents; and electronic data e.g. customer, order, salary information, etc.

Although in many SMEs **information is the main capital**, often insufficient attention is paid to the management and protection of information. To operate successfully, a company should ensure that:

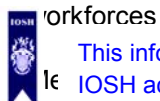
- Information is correct, reliable and up to date
- Information is always accessible by the right people
- Information doesn't end up in the wrong hands

Information losses or leaks can be both distressing and damaging!

The changing world of information risk

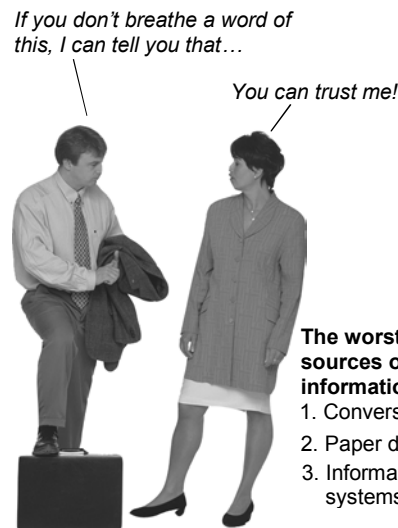
The world of information risk is one of continuous change. In all fields, business life increasingly involves information processing – documents and knowledge are constantly transferred and processed in more and more varied ways and through increasingly complicated networks.

- Information moves in new ways through company networks
- Employment periods may be shorter – are these employees less committed/loyal?
- Viruses are a threat to text documents
- Cultural/social factors need consideration when dealing with international customers, suppliers or



This information is provided in good faith, however it is not comprehensive and OSHA accepts no liability for any losses incurred from its use, howsoever caused.

- Where do you speak on your mobile phone?
- On the Internet, the whole world is your neighbour



The worst sources of information leaks

1. Conversations
2. Paper documents
3. Information systems

- Electronic business will change trade and payments traffic

Management of information risks

The management of information risks starts with identifying the main hazards related to information. An information risk chart can be found on the back of this card. After the main problems have been found, more in-depth hazard identification and risk management work is implemented with the aid of the work cards included in the Toolkit. In risk management, the development of a company's operations (modes of operation, expertise and management) should be chosen as the starting point. Technical means of protection only come after that.



Information Risk Chart

| | |
|-----------------------|-----------------|
| Company: | Group/Assessor: |
| Object of assessment: | Date: |

Management

- Management awareness of the significance of information risks
- Identification of the most important information
- Awareness of the biggest risks
- Information security policy and practice
- Information security as a part of the quality system
- Company has access to sufficient expertise
- Development of information security activities
- Others

Protection of information systems

- Responsibility for systems
- Paper handling
- User rights
- Remote working
- Monitoring of operation (failures, use, disc space)
- Archiving and document handling
- Management of change
- Removal from use
- Software procurement
- Backups
- Passwords
- Extranet and www
- Others

Activities of personnel

- Training in information risk management
- Information security policy
- Clear instructions
- Actions at the end of employment
- Management of user rights
- Preparations for failures and accidents
- Protection of individual equipment (e.g. anti-virus software etc.)
- Others

Information Risks

Premises

- Exposure to accidents
- Shared occupancy premises (partitions etc)
- Access control
- Guarding and security against break-ins
- Partitioning of premises and access rights
- Archives and document handling
- Fax machine/printer etc.
- Customer space
- Others

Business relationships

- Security classification of network partners
- Common rules
- Risks from subcontractors
- Surveying of different parties
- Agreements
- System user rights
- Information security during negotiations, etc.
- Protection of shared information
- Others

Example of use

Agreements – a significant risk **OK** Access control – issue in order ~~Passwords~~ – does not concern us

Management. Management awareness and control of information risks is the foundation of information risk management. Practical management tools include controlled-information security procedures, the use of expertise, the integration of information security and quality systems, etc.

Activities of personnel. Information risks are either managed or realised through the practical actions of personnel. Expertise and procedures create a foundation for success and employees must be adequately trained. Effective tools for risk management should be provided for personnel e.g. automatically operating anti-virus software.

Premises. Accidents and theft are key information security risks. Access control, partitioning etc. are basic control measures for managing these risks.

Protection of information systems. The protection of electronic information systems is one of the main challenges of information risk management. However, the management of paper-based systems is equally important.

Business relationships. Information risks in business relationships are accentuated through networking and subcontracting. The adequacy of the information security systems of the different parties should be assessed and classified. Training and monitoring should be used to ensure that there are no weak links in the network. Trust must work equally well in all directions!