Risktopics

ZURICH

April 2011
Country of Origin: United Kingdom

Protection of Computer Data and Software

Introduction

With business dependence on computer systems, the question of protection to computer data and software is of paramount importance in relation to the physical aspects such as fire, heat and water damage. In addition, care needs to be exercised to guard against the potential risk of corruption and/or manipulation of data and software, the consequences of which could have a significant influence on the day-to-day efficiency of a business. More recently, the protection of the personal data of customers and employees has become increasingly important with developments such as the Data Protection Act 1984 and the much broader Data Protection Act 1998 and the significant rise of identity theft, fraud and similar criminal activities.

Computer Data and Software should be protected to a degree appropriate to its importance. Staff vigilance and compliance to a data security strategy is vital for achieving suitable levels of protection. In order to achieve this, management should appoint persons to be responsible for maintaining such a strategy.

The following guidelines have been designed to assist in providing and maintaining safety precautions to avoid physical damage, corruption and theft of computer data, personal data and software.

Responsibilities

Senior management should take overall responsibility for the protection of data and should define the accountability and responsibilities of staff within the organisation. This should form a management authorised document clearly stating total security policy, objectives and commitment and should take into account all aspects of the Data Protection Act.

Responsibilities should be compatible with other fire and security measures, in order to ensure there is no conflict of interest with regard to the overall security arrangements.

Procedures should be clearly defined for staff assuming responsibility of the computer system upon discovery of corruption to either data or software or breaches in the company security policy which could result in theft or misuse of company or personal data.

User Control

A workstation could comprise a computer terminal, desktop PC or a portable device such as a laptop. All of these workstations provide potential access to all information stored in the workstation and as such it is necessary to ensure that the workstation usage is properly authorised and controlled, using physical and software controls as outlined below:

Access to Workstations

- At each workstation location an individual should be responsible for authorising access to the workstation.
- Measures should be taken to avoid illicit viewing of confidential or restricted data. These might include the installation of workstations in controlled areas and automatic screen clearing after a specified period of keyboard inactivity.
- Communications lines, sockets, patch panels and switches should be physically secured and accessible only by authorised personnel.
- Physical inventories of workstations (including personal computers), communication hardware and magnetic media should be carried out at all remote sites to check that only authorised equipment is used.
- Laptop security procedures should be established when laptops are taken out of the office i.e. they should not be left unattended, or if left in a car should be locked securely in the boot and not left on display. Ideally, when left in offices overnight they should be locked in suitable drawers or cabinets.
- Consideration should be given to the protection of high value computer equipment with physical security devices such as security cages, anchoring bars or security cable locks.
- Visitors, delivery companies and contractors coming onto the premises should be properly supervised with suitable access control arrangements established for the reception of the property and for other entrances/exits.

Software Access Controls

- Consideration should be given to the provision of physical security devices to prevent access to computer data and software such as dongles or USB port blocker devices.

- Security of software should include features which deny access to all or part of the system. A password is a commonly used means of allowing computer systems to recognise an authorised user. Passwords should be unique to each individual. Group passwords should not be used.

- Passwords should be of a complexity commensurate with the sensitivity of the access and should consist of at least 6 characters of an alphanumeric mix, where possible. Passwords should be kept secret. In no circumstances should they be centrally displayed or details left beside terminals.

- It is suggested that passwords are changed as follows:

    - At regular intervals, at least monthly, or after a specified number of log-ons.

    - If the user leaves employment or is transferred to another department.

    - When the password has been revealed to others.

    - If user behaviour necessitates a change.

- Failed access attempts should be signalled at operator consoles as they occur. Security staff should investigate regular failures and denials.

- Access authorisation for engineers or outside maintenance persons should be cancelled on completion of their task.

- Management should ensure that all users log-off when leaving a terminal, even for relatively short periods. Where possible, terminals should log off automatically after a predetermined period of key inactivity (e.g. 5 minutes).

- Acquisition procedures for software should be established to ensure that software used is reliable and from a reputable source. No unauthorised acquisition of software or other downloads should be permitted. Acquired software should be checked with appropriate virus checking facilities before being introduced to the main computer systems.

- All computer systems and laptops should be protected with good quality anti-virus software, which should be updated regularly.

Storage of Data and Software

The following guidelines provide best practice advice for the safe storage of data and software

- Procedures regulating access to stored data should minimise the possibility of unauthorised viewing, use and corruption by modifying manufacturers' standard file names.

- A procedure should be in operation to ensure that back-up copies of data and software are made and regularly up-dated (e.g. daily or weekly) as required.

- All back-up copies should be checked for validity and should be readily identifiable.

- Back up copies should ideally be held off-site or kept within an approved fire resisting cabinet, providing a minimum two hour fire rating. The following details shows critical temperatures above which media will become damaged from the effects of heat:

Hard Disks	65°C
Magnetic Tape	65°C
Floppy Disks	52°C

- Short term off-line back-up media, where a high level of availability is required, should be stored in security controlled areas.

- Stored data should be deleted when no longer needed. Periodic audits of the data stored should be carried out to ensure no redundant data is being kept unnecessarily.

- Where appropriate, data should be encrypted, in particular, where data is being stored on portable memory devices such as CD ROMs, USB memory sticks or similar devices to be taken out of the office.

Printed Data

Where data is reproduced on paper, or where written data is to be presented for input to a computer it should be afforded the same security precautions as for stored data. Sensitive printed data, for example, should be stored in security cabinets.

Printed data produced for drafting or information should be destroyed (shredded) when no longer required. Operators without the appropriate authority to process information of a certain data classification level should not be given the task of destroying printed data.

Personal Data Security

The prolific rise in a variety of cyber based criminal activities and other frauds including identity theft and similar crimes has resulted in businesses having to pay more significant attention to the security of the personal data of their customers, employees and other third parties held on their computer systems. The Data Protection Act 1998 covers how information about living identifiable persons is used and is much broader in scope than the earlier 1984 Act. This Act makes clear demands upon organisations in terms of the security that must be applied to protect personal data. Failure to adequately protect personal data can result in prosecution under the Data Protection Act and significant fines or penalties. The following guidance is designed to minimise the risks from loss of personal data:

- A formal security policy should be introduced to clearly identify what information held regarding your customers, employees and other third party individuals is considered personal data under the Data Protection Act. Ideally, personal data held on your computer systems such as names, addresses, bank details and medical information should be categorised. Categories could include highly confidential, confidential or internal only. The security policy should highlight the responsibility of all employees under the Data Protection Act to ensure the security of personal data held on your systems and this policy should be actively communicated to all employees.

- Access to personal data held on the computer systems should ideally be tiered, with access to databases (and other applications) containing highly confidential personal data such as medical information being restricted to only certain employees with password security features as appropriate.

- Physical access to server or communications rooms should be restricted to only authorised employees with doors being kept locked, either by conventional locks or, preferably by electronic access control systems which allows a log of all activity through the door.

- Specific procedures should be established for protection of personal data taken out of the office. For example, laptops should be password protected and not be left unattended and data on USB memory sticks or CD ROMs should be encrypted.
- The computer systems should be appropriately protected from external interference and hacking. They should be protected by suitable “firewall” software and anti-virus protection including “spy ware” software.
- If terminals or laptops at physically remote sites such as homeworkers premises require access to the main network, a permanent connection to the network should not be used. Remote terminals should be automatically locked out after a set period of time. Suitable password security, to allow connection to the networks, should also be provided.
- Any obsolete or redundant computer terminals, laptops or data storage devices such as USB memory sticks should be properly purged or wiped of personal data before being disposed of. Procedures should be put in place for equipment to be returned to a central point to enable hard drives to be wiped by specialist contractors or employees.
- All employees should be actively encouraged to report breeches of the security policy and there should be formal procedures established for how to report and deal with breeches in the security of personal data.

Summary

Due to the increased reliance on computer systems for more and more aspects of running a business, any loss of computer software and data is likely to seriously affect your business. This may not only result in additional financial costs to restore software or data and potential loss of production but may also result in damage to your business reputation and a loss of confidence by your customers. In addition, breeches in the Data Protection Act can result in prosecution and heavy fines or sanctions. Therefore, it is important to properly protect all software and data provided on your computer systems. The guidance in this Risktopic is not intended to be exhaustive but is presented to highlight the main issues and concerns in order to minimise the risks of software and data loss.

Useful References

1. FPA InFiReS guidance RC3c - Recommendations for loss prevention in EDP and similar installations Part 3: Protection of Data and Software.

CONTACT

Risk Engineering
Risk Support Services
126 Hagley Road
Edgbaston
Birmingham
B16 9PF

Phone +44 (0) 121 697 9131
www.zurich.com

For more information please visit:
www.zurich.com/riskengineering

Zurich Management Services Limited, Registered in England and Wales no. 2741053, Registered Office:
The Zurich Centre, 3000 Parkway, Whiteley, Fareham, Hampshire PO15 7JZ