



Physical Security of ICT Equipment

Business Office Equipment

With the wide range of IT equipment now available on the market, there is an equally vast array of security solutions available to secure your equipment. What follows here is a broad selection of what is present on the market and tips to help reduce the threat of crime.

High-value equipment, such as computers, monitors, projectors, printers etc, are key targets for burglars. When you are choosing the correct security system for your needs it is advisable to ask your insurance company whether they have a list of approved suppliers. In some cases, reduced premiums can be obtained. Many of the things for consideration on this page should be included in the company security policy. Please see the pages on security policies for more information.

Chains, cables and locks

Haspers, cables, lock-down plates, lockable clamps etc. can be used to secure equipment to an anchor point like a solid surface or structure. They will prevent 'smash and grab' incidents, especially by opportunist thieves. Items such as laptops and projectors can be securely fastened to desks and are especially useful in areas such as offices & libraries, where the owner can feel safe leaving the equipment unattended for short periods of time.



These offer the flexibility to secure equipment temporarily if it needs to be moved around on a regular basis. Under-desk mounting reduces visibility and access to the cables.

Reducing equipment visibility

Wherever possible, try to place office equipment out of view from passers-by, or install blinds or light-reflective film to reduce visibility. Opportunist thieves (or even those stealing to order) are less likely to try and access your premises if they are unable to view the equipment you have on site.

Cages and boxes

Enclosure systems are available that deny access to any part of the computer once it is locked. They provide partial or total encasement, and are bolted to the desk or floor providing ideal security for servers. If you want to protect software or storage devices then locks that cover drives are available.



Servers and server rooms

Servers should be kept in well-ventilated, dry cabinets or security cages, preferably in an internal room that only provides access by coded or British Standard lock. This not only reduces the risk of theft, but also the risk of accidental damage through overheating or of the server being tampered with during the working day. The potential loss of data through damage to the server could be more costly than the damage caused by theft.

Laptop computers

All offices should try and operate a 'clean desk' policy in that all equipment should be locked away in a secure place whenever possible. As discussed later all laptops should be properly security marked.

As this type of equipment is designed to be used away from the office, it is necessary to consider how the equipment will be stored when away from the office and the condition in which it will be transported. Guidelines on use and storage should be given to all staff that use portable equipment to make sure theft and potential damage is limited.

Employees should be told clearly not to leave equipment such as laptops, mobile phones etc on view in their vehicles at any time, even for short periods. Equipment should be taken with them or secured in the boot - excellent boot storage boxes are available for use in vehicles.

If in the case that company equipment is left unattended in vehicles or whilst away from the office then the company should consider using penalties against staff. This is especially the case if the item contains sensitive client data as the company itself may be liable for a hefty fine.

The company may also want to consider tagging equipment. Tags can be placed on chipboards inside the equipment that trigger alarms when they are taken without authority.

Mobile phones and PDAs

Mobiles, PDAs (palm-tops) and similar items are often targeted by robbers, particularly when they are being used in vulnerable locations. Areas such as car parks are the biggest crime spots as thieves prey on the fact that employees leave equipment unattended in their vehicles. There is no excuse for not putting these items in your pocket and carrying them with you even while you are working in an office.

Record the details of your phone or palmtop such as the make, model, phone number, and (for mobile phones) the IMEI number. The IMEI number is a 15-digit number unique to each mobile phone handset. It can be obtained from most handsets by typing *#06# into the keypad. If your phone is lost or stolen, contact your service provider as soon as possible so that they can block its use. Most mobile phone companies and network providers now offer a service where they will hold all the telephone numbers stored in your phone for easy retrieval should it be lost or stolen.

Marking your equipment

All equipment should be clearly marked with identity codes both on the main shell itself and internally. In some cases it is not necessary to mark equipment clearly and blatantly and for these situations there are methods for marking items in invisible, uniquely identifiable and irremovable methods.

Replacing stolen equipment

It is important to be aware that you are more likely to suffer theft if you have previously been broken into - the thieves know you will probably have replaced the equipment they stole previously. Always make sure that the necessary security measures have been put in place before you replace any equipment. After all, if the criminals have found one weakness to get into your business, they may easily be able to find another!

Contact the Business Crime Reduction Centre
on 0114 275 1283 or visit our website at www.bcrc-uk.org

Business Crime Reduction Centre, working with South Yorkshire Police to reduce crime against business

Business Crime Reduction Centre
4th Floor, Castle Market Buildings, Sheffield S1 2AH
Tel: 0114 275 1283 Email: info@bcrc-uk.org