

The cost of PC theft to you!

Statistically, the average cost of PC theft in the UK is in excess of £25,000. Companies who self insure obviously have to meet the full cost of any loss, however even where insurance is in place, it is estimated that in over 75% of incidents the victim company still has to meet at least part of the cost directly.

Costs often not covered by insurance include; any excess on the insurance policy, software rebuilding costs, costs associated with lost business or delays in invoicing customers. In addition to the financial implications the inevitable disruption to work-flows often makes theft a very traumatic experience as well.

Theft of a PC will also probably involve loss of data (i.e. as stored on the hard disk) which may be company sensitive and therefore a threat to the continued operation of the business. If personal data were stored on the PC, the theft could even render the owner

liable to personal prosecution under 'Data Protection' legislation, although the use of data encryption systems or the installation of a PC immobiliser system such as PC Access may offer a solution to this problem.

With a little thought and modest expenditure however there are a number of things which can be done to reduce the risk of theft.

Cost effective solutions

Sadly any security measure can be overcome given adequate knowledge, resources and time, and as evidenced by one company in the midlands (burgled three times in two weeks), even companies with on site security guards, closed circuit television, and monitored intruder alarms are at risk.

The most effective form of security is often achieved by using a combination of security systems and products implemented in such a way as to form a number of layers of defence each designed to:

- Delay and / or detect the thief on site thus increasing the risk of apprehension
- To reduce the value of the goods stolen, or to increase the risk of the thief being caught whilst trying to dispose of the goods.

Choose the best options for your environment

The security measures described in the following pages have been proven to be effective in use when properly implemented and used in conjunction with other measures such as normal building security. Although generally supported and recommended by Police and Insurers, as with all security measures the ultimate responsibility rests with the purchaser to ensure that the options chosen are appropriate for the environment in which they will be used.

Physical theft deterrent systems

A number of inexpensive products are available to physically restrict access to, or prevent the unauthorised removal of individual items of equipment. Designed for use in conjunction with existing building security measures, when installed and used properly such products offer an excellent second line of defence against the thief and your Insurers or local Crime Prevention Officer will be pleased to offer advice on what may be suitable for your environment and to provide details of reputable suppliers. For convenience it will be helpful to consider the available options under the following sub headings:

- Secure containers
- Direct attachment devices
- Security cable and chain systems.



Secure containers

Safes and locked cabinets can be used to protect equipment against theft, however these units generally offer no more than a secure overnight storage area for equipment and are therefore of limited practical use as the physical action of repeatedly plugging together and unplugging electrical connectors is likely to result in early failure of the contact points. Specialist 'enclosure' systems for items such as PCs and video recorders are available at a fraction of the cost of a good safe, and will typically allow such items to be secured in place in a way that prevents unauthorised removal of the equipment but allows access to all main controls even whilst the unit is secured. Enclosures are normally designed to attach directly to the desk or floor via screw or bolt fixings, although mobile trolley type multistorage modules for laptops are becoming increasingly popular. An obvious advantage of a specialist enclosure system is that in addition to the equipment being secured against unauthorised removal, access to internal components (such as high cost PC expansion boards, memory, etc.) is also prevented.



Direct attachment / lock down plate and rail systems

In its most primitive form this could mean simply bolting through the computer casing and the work surface. However commercially available lock down plates and rail lock systems can avoid damage to desk surfaces or equipment casings, should not impact on the equipment manufacturers warranty and will make subsequent relocation / replacement of equipment much easier.

Normally lock down plates are in two parts which interlock. Unobtrusive pads are attached (with special adhesive) to the base of the computer and then the pads, similar to large feet can be bolted to the top part of the base plate. The bottom part of the base plate can be fixed to a secure surface, be it to the top or side of a substantial piece of furniture like a desk, or to the wall or floor, by a variety of means most suited to the

particular location / surface. Typically bolting through or into the receiving surface provides the best security (e.g. coach bolt fixing through desk tops, anchor bolt fixings into concrete floors,) whilst adhesive fixings may be appropriate in some cases and can be used as an alternative in order to avoid damage to the receiving surface (e.g. a desk top). Once secured the two parts of the plate are interlocked and held together with a locking mechanism. A well designed lock down plate or rail system will ensure that all fixings are protected when the system is installed and locked, that equipment relocation / replacement is kept simple, be available in a range of sizes and will allow peripherals to be secured using low cost cable extension systems.



Security cable and chain systems

This form of security offers cost effective protection against the opportunist thief, but little

defence against organised gangs of thieves who will almost certainly arrive armed with substantial cable/chain cutting implements.

Cable systems are also used in some public areas (e.g. within airports, local authority offices, etc) to secure equipment to desks and as protection for staff (to stop equipment being hurled at staff by frustrated or irate members of the public). A further benefit of cable systems is that they prevent the unauthorised relocation of equipment within an organisation thus becoming an integral part of general asset management.

Cable systems are popular because of their low cost, the fact that they are easy to self install and they allow a certain amount of movement of the secured item. Where equipment is frequently moved, this form of security is often the owners preferred choice and in the case of items such as portable and notebook computers there are limited practical alternatives (see also Protecting laptop computers).

With cable systems, normally each item of equipment to be secured is fitted with a special security bracket or attachment, which is used to secure the

equipment to the security cable. The cable is then secured to an anchor point, which is itself fixed to the building structure (i.e. wall or floor) or possibly to a substantial item of furniture. Whilst many commercially available systems incorporate general purpose attachments / fixings which are offered for use with any type of surface, the more professional systems include specialist fittings and will be offered with a range of easy use adhesives / fixings designed to offer a secure fixing to the most commonly encountered surfaces. Attaching an anchor point to a wall obviously requires a different type of fixing than a unit to be fixed to a desk surface for instance, and the desk fixing will be totally unsuitable for attachment to a computer casing and vice versa.

From a security point of view there is little to choose between a cable or a chain based system. A plastic sheathed steel cable will cause less wear on equipment casings and tends to look more attractive. Some cable systems allow cables to be locked securely into a locking point with an integral locking mechanism whilst others rely on a padlock .

Smoke generating and alarm systems

Smoke generating systems

The use of smoke in warfare to obscure a target for instance, is well known and dates back to 2700BC, however there are now commercial systems on the market which can be used to generate it. Within seconds a dense blanket of fog fills the room, thus protecting equipment and other items of value against theft (thieves can't steal what they can't see!).

There is no doubt that such systems can be very effective, especially for protecting equipment store rooms, etc. These systems are however not appropriate for all locations and installation must be carefully planned and professionally undertaken. Quality components, careful location, failsafe mechanisms / isolator switches, notification of

interested parties (Fire Brigade, Police, Alarm Companies), are all fundamental to a safe installation.

Local alarm systems

The main function of an alarm is to alert someone to the fact that something is wrong and that some form of action is required. By definition therefore the availability of someone to 'Take Action' is implied, a factor often overlooked when deciding to install ad hoc alarm protection. Used correctly alarm products offer a real benefit, however professional thieves are unlikely to be deterred by such devices and are often able to deactivate such units quickly. Alarms which run continuously can cause unnecessary distress and could lead to prosecution for 'nuisance'. Ideally alarms should self terminate within an

appropriate time period of being triggered although they should be designed to immediately rearm themselves again after resetting and may re-trigger should the sensor(s) be re-activated. Local alarm systems fall into three general categories:

- Local entry warning alarms
- Loop alarm systems
- Alarms installed in or on equipment.



Local entry warning alarms

Free standing door / window alarms are available which are typically triggered either by some form of contact being broken (i.e. a magnetic contact or reed switch), or alternatively by sensing movement, heat or vibration (some units incorporate more than one form of sensor to eliminate the possibility of false alarms). Local alarm units are normally battery powered, are typically stuck or screwed to a door or window frame, and emit a piercing



oscillating siren in the 90-130db range when triggered. Door alarms are available with various features and levels of sophistication. Some can be set to announce visitors with a gentle chime, many incorporate a delay trigger feature which may for instance be used to alert staff to the fact that fire doors have been left open. Control mechanisms normally involve either physical key operation, or codes entered via a numeric keypad. (Warning – many very low cost units incorporate low grade components and are of poor quality manufacture. Such units are likely to be unreliable and / or prone to early failure).

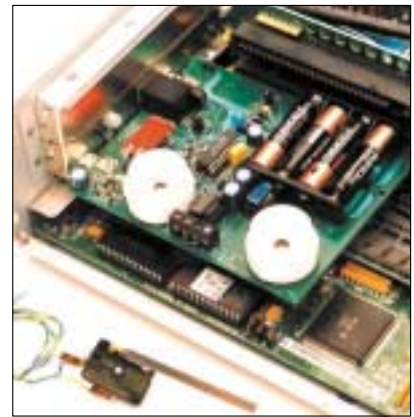
Loop alarm systems

Most people are familiar with the type of alarm systems used in retail outlets to protect goods on display. Similar systems can also be used to protect equipment in the office environment, where typically they will trigger a local alarm siren on activation. This type of installation can be cost effective, and there are now even some plug-n-go type systems available that lend themselves to easy DIY installation. These systems may be battery powered, but more typically will be mains powered (with battery back up for alarm integrity).

Alarms installed in or on equipment

Such alarms normally take the form of movement detectors and will typically incorporate either some form of ‘trembler’ sensor or alternatively a ‘mercury (tilt switch)’. Better quality units incorporate anti tamper circuits / protection to prevent unauthorised de-activation. Typically these alarms will be powered either by a rechargeable battery (which itself is trickle charged via the equipment power source) or via a stand alone battery. Stand alone battery (alkaline or lithium) driven models offer the advantage of allowing the alarm circuitry to be fully isolated from the equipment electronics. Care needs to be taken when purchasing alarms which use rechargeable batteries (particularly it appears those employing shrink wrapped button cells) as rechargeable batteries have been known to explode during charging – obviously a potential danger where such units are incorporated into internally mounted PC alarms.

Internally fitted units may require professional installation, and although unlikely, could possibly invalidate the equipment manufacturers warranty.



Externally mounted units will not normally require professional installation, neither should they impact on warranties. They are however obviously more easily deactivated or muffled by any would be thief than internally mounted units.

Such alarms vary wildly in respect of both manufacturing and component quality and the purchase of better quality units is strongly recommended for this type of application.

Marking your property with your company name and post code may discourage the opportunist thief and will certainly assist the Police to return your stolen goods should they be recovered. Conventional property marking systems fall into two main groups, covert marking and visible marking, although more recently software based systems have become available for use with PCs.

Property marking systems

Covert marking systems

U/V marking, microdot marking such as the 'Alphadot' system, 'Smart Water' type products and various passive electronic tagging systems. Such systems act as a deterrent, as unless any would be thief can be sure that all marks or tags have been removed, the stolen item could be traced back to the genuine owner and prosecution could follow.

U/V marking has largely been overtaken by newer more effective technologies and as the marking fades with time and exposure to light it needs to be refreshed periodically (e.g. every 6-12 months). A new generation of permanent U/V markers have evolved to prevent removal of the mark with water or solvents, however even these marks will still deteriorate over time with exposure to light.

Whilst many of the passive electronic tagging systems

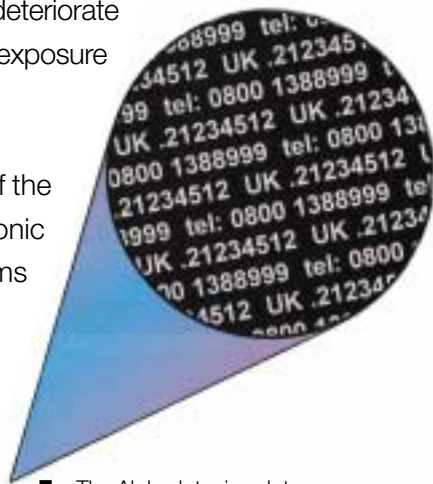
are good products, generally speaking each system requires a special reader to identify the content of its tags which tends to place a practical limitation on their effectiveness (see Tagging systems).

Visible marking systems

Indelible ink marking, stick on labels, chemical etching systems, engraving and hot branding systems. Label based systems often incorporate sequential numbering and can therefore be used for asset register purposes in addition to the identification / security application. Some label systems incorporate a stencil cutout of the postcode or company name through which a permanent mark can be engraved into the equipment

casing to which the label is bonded. Chemical etching systems are popular, being among the cheapest options available. Engraving systems are cheap to use however freehand marking is seldom attractive and use of some form of stencil or marking template is strongly recommended. Hot branding can be effective, however is generally only suitable for use on plastic surfaces and for professional results needs to be undertaken by a skilled operative.

The low cost involved in marking your property makes it a worthwhile investment, however it should be regarded as additional protection and implemented in conjunction with other security measures.



[•] The Alphadot microdot measures just 1mm in diameter yet contains a unique pin number and Traceline database phone no.



Software based marking systems

Installing a covert tracking system such as WebDetect on a PC could act as a deterrent to would be thieves and could aid recovery of the PC and prosecution of the thief in the event of the PC actually being stolen.

Tagging systems

A familiar feature in the high street, tagging systems are used to protect a wide range of goods in the retail environment from compact discs to leather coats. Typically tags are enclosed within the packaging of, or are securely attached to products on display. Normally an alarm is triggered at the sensor station (located at the exit) should someone try to leave a shop with goods where the tag has neither been deactivated or removed.

Such systems consist of two major components, the tagging device and the sensor unit, and



generally utilise magnetic or radio frequency technology for their operation. Tagging devices will either be in a permanently 'active' state, or may be 'passive' until activated by coming within range of a sensor unit. Retail style tagging systems do not lend themselves easily or cost effectively to securing operational equipment such as PCs in the normal office environment.

Other forms of tagging systems include small data storage tags which can be concealed inside equipment casings and which can typically store up to 1 megabyte of data and a uniquely identifiable registration code thus enabling stolen equipment which is subsequently recovered to be returned to its rightful owner. Although conceptually good, these systems rely on the use of special reader/sensor equipment which may not always be readily available, (especially as generally each system requires its own specific reader device to decode its tags).

These systems also typically rely on access to some form of computerised central database where details of registration or ownership are recorded, and there is periodically concern



expressed about the implications of Data Protection legislation in respect of passing out information extracted from such databases (even to the Police).

A new generation of RF (radio frequency) based tagging and asset control systems is currently emerging. As with any RF based system the effective operational range of the transmitter / receiver will be effected by the surroundings, the materials used in and the construction of the building, however sensor detection is possible at ranges of up to several metres in most normal buildings.

Advances in available technologies coupled with significant cost reductions in many areas of high tech manufacturing heralds a new era for electronic tagging and tracking systems.

Given the potentially new and rapid developments in this field it will be advisable to check on current offerings at an early stage of any evaluation process.

PROTECTING LAPTOP COMPUTERS

Laptop computers have a high initial value and are popular targets for thieves. They command a high second user value as they are readily disposable on the second hand market. In all probability a stolen unit will also have at least some company sensitive or personal data stored on the hard drive which could be embarrassing or commercially costly should an external party gain access to it and could possibly even lead to prosecution under the Data Protection Act.

Physical anti theft measures include cable lock down systems, desk cradles and secure storage cabinets (for storing multiple units), whilst portable alarm systems can also be used to identify unauthorised movement of the equipment.

Installing a covert tracking system such as WebDetect on the PC could act as a deterrent to would be thieves and could aid recovery of the PC and



prosecution of the thief in the event of the PC actually being stolen.

Preventing unauthorised use of the laptop and protection of the data stored on the PC hard drive, can be achieved via use of a PC immobiliser or access control system.

PROTECTING YOUR DATA



Storage and protection of data media such as CDs, backup tapes and discs, is best achieved by using a purpose designed data safe. A data safe is designed specifically to protect data media against a range of hazards including fire damage, humidity and electro-magnetic contamination. Note, a fire safe or burglary safe should not be used for storing data as they do not offer appropriate protection. (See [‘Choosing a safe’ page 34](#))

Disc drive locks and CD-ROM locks provide a simple yet effective physical means of preventing the unauthorised use of floppy disc drives, tape or CD drives, for the downloading of data from a PC. It should be remembered however that other measures must also be considered especially in networked PC environments or where PCs are connected to the internet.

Other products which can help protect against unauthorised access to or use of the data on a PC's hard drive include: PC immobiliser / access control systems (including password free systems) and data encryption systems.