



RISK MANAGEMENT GUIDE

PREVENTING THEFT OF COMPUTER AND OTHER ELECTRONIC OFFICE EQUIPMENT

What is the scale of the problem?

Theft of computer and other electronic office equipment is amongst the most widespread and costly crimes affecting the business community. Due to constant technological advances and the demand for ever more sophisticated equipment, it is likely that the problem will continue for the foreseeable future.

Computers and other electronic office equipment are now essential parts of business life and their loss together with the loss of data and software held in machines can have a devastating effect on small and large organisations alike. Even though insurers can provide compensation for the direct consequences of a loss, the victim may have to bear the costs of missed business opportunities, reduced customer service, lost time and reduced staff morale.

Some criminals do not target complete machines. The components within some computers have such a high value in relation to their size that there are occasions when thieves remove the electronic parts such as processor and memory cards and chips leaving the remainder of the computer on site. A single bag or box of components can have an equivalent retail value measured in hundreds of thousands of pounds.

Aside from computer hardware, there is evidence to suggest that thieves are now also targeting computer software. These computer programs, which include CD-ROMs and Office software packages, are attractive due to their relatively high value, their portability and ultimate re-saleability.

Threats of or actual violence to staff is another worrying development. Close attention must be paid to the control and supervision of access to the premises, especially during times of reduced occupation such as at opening or closing times, lunchtimes and during night shifts. Particularly at risk are computer component manufacturers, stockists and distributors, and users of servers and PCs containing costly high-powered or specialist components such as those used in the telecommunications, media, financial, medical and further education sectors.

It has also been shown that a victim of computer theft has a very significantly increased risk of suffering another theft, usually within 3 months, and often within a few days or weeks of the initial loss i.e. when the thieves expect the original equipment has been replaced. Implementation of a package of measures, at the very earliest moment following a burglary, would dramatically reduce the likelihood of repeat victimisation.

Equipment owners and users run serious risks of theft and damage unless positive steps are taken to deter criminals. The precautions outlined in the following pages can help prevent or reduce losses and in combination have been shown to be a very effective deterrent against theft.

It is important to note in this context that many insurance policies contain specific Conditions (for example Minimum Security Standards) relating to loss prevention and risk reduction measures. Where these apply, they must be met in full.

Disposition of Property

Careful siting within the premises can reduce the vulnerability of target property. Time is the enemy of the thief and an immediate benefit accrues if the equipment is placed away from the perimeter and beyond obstacles that slow and frustrate progress of theft such as staircases and locked internal doors.

Physical Security to Premises

At the very least, the building perimeter doors (other than fire exits) should be secured by a British Standards approved BS 3621 or equivalent mortice deadlock or (unless it is the final exit door) two internal key-operated bolts. All accessible windows should be secured by key-operated window locks (unless they are designated as a fire exit).

This is the most basic of security standards for any commercial premises but the level of theft attraction inherent in this property is such that much stronger barriers are desirable. The need for steel linings, bars, grilles and shutters to doors and windows or replacement with proprietary intruder resistant products may be unavoidable in order to slow the progress of the more determined gangs. You will be advised what level of protection is required to your premises at the quotation stage or if applicable, following a survey of your premises.

Intruder Alarm Protection

In addition to physical security, your business premises may need to be protected by an intruder alarm system depending on a number of factors including your sums insured. You will be advised what level of protection is required for your premises at the quotation stage or if applicable, following a survey of your premises. If an intruder alarm is required it must be installed and maintained by a company which is acceptable to the police and is recognised as an installer of intruder alarms by either the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB).

We will work with you to establish the exact requirements and specification of your alarm system, for example your premises may require an 'audible only' system or a more sophisticated system that is capable of automatically alerting the police to a break in.

Lockdown Enclosure and Entrapment Devices

Devices, such as lockdown enclosures and entrapment devices, should be used to physically tie down equipment such as servers, central processing units, personal computers or printers. They can either be held secure with industrial adhesive or preferably bolted to workstations, floors or walls, and are suitable for equipment that is not required to be frequently moved.

Evidence suggests that the most effective securing device is the retaining base plate of the "enclosure" or "entrapment" type designed to prevent access to components as well as theft of a complete unit.

Cable-restraint products offer less protection than the lockdown/enclosure device which should always be the first choice for target items such as servers and central processing units.

The effectiveness of the product largely depends on the diameter of the steel cable and it is important to ensure the anchorage points and locking arrangements are of comparable strength. Where possible, the cable should be installed in a manner that also helps to prevent theft of the equipment components.

Devices should not be purchased until confirmation has been obtained from **MORE TH>N BUSINESS** that they meet their insurance requirements or recommendations.

The Loss Prevention Council has published a standard - LPS 1214 - 'Physical protection devices for personal computers and similar equipment' and the Loss Prevention Certification Board certifies products against this standard. Products that have been successfully tested should give users the confidence of knowing that they meet set standards of resistance. In particular, those certified to Category 2 will provide a higher level of protection. However, a number of Category 1 devices also offer a good standard of entrapment protection, and these are generally to be preferred to those which offer whole unit restraint only.

Before fitting a lockdown, enclosure or entrapment device, care should be taken to ensure that it will not affect the equipment manufacturer's warranty or any hire or leasing agreement.

Custom-made steel-mesh security cages and sheet-steel enclosures are also available for larger units.

Although devices are available for securing laptop products, these are best locked away in secure cupboards (or, better still, safes) when not in use, and in a car the laptop should be kept out of sight in a locked boot.

Protecting Laptop Computers from Theft

The increased use and ownership of laptop computers has been accompanied by a rise in theft because they are easy to steal and open to opportunistic theft. Apart from the loss of the hardware there may be the loss of sensitive commercial information which is of a far higher monetary value than the laptop itself. Where users have been given a strict responsibility for the security of their laptops, the incidence of theft and loss can be reduced significantly.

Actions to prevent opportunistic theft and theft by collusion:

- Have an inventory system which requires individuals to sign for a specific laptop, whether for use inside or outside the office
- Make sure that equipment is not swapped or lent to other staff without proper authority
- Ensure that arrangements are made to retrieve a laptop when an individual leaves the firm
- Ensure that staff are aware that theft, whether internal or external, will be reported to the police
- Consider whether loss by gross negligence should result in disciplinary action, perhaps the imposition of a fine
- Clearly label or postcode mark equipment
- Lock equipment in secure cupboards (or, better still, safest), even during office hours when it is left unattended
- Secure meeting rooms when equipment is left unattended
- Use access control systems to limit access from public areas such as receptions, factories or warehouses to the main office facilities, and encourage staff to challenge unfamiliar visitors
- Reduce the likelihood of street robberies by disguising carrying cases used to transport laptop computers
- When travelling by car, lock equipment which is not being used in the boot.

Keys

Keys to securing devices should be kept in the custody of authorised personnel only and either removed from the premises when they are left unattended or placed in a locked safe (the keys and/or notes of combination number to be removed from the premises when unattended).

Alarm Devices for Individual Items

These are primarily designed for daytime protection and are suitable for premises that have a constantly manned reception or security desk. It should be appreciated that the devices do not physically restrain the equipment and that the security they provide outside business hours is limited if there is no immediate on-site response.

Property Marking

To be truly effective as a deterrent, property marking must be permanent and prominently displayed. In practice, this generally means etching or branding a postcode and company name (or logo) into the equipment casing preferably in more than one location. The marking should be of such size and in such position that its existence cannot be overlooked and its removal or concealment would prove very difficult. Some marking systems can incorporate sequential numbers that can identify individual machines or workstations and can be a useful part of asset control procedures. Where applicable, owners and users should consider whether marking might affect their warranty, hire or leasing agreements.

Access Control

Bearing in mind that many losses involve equipment stolen during working hours, access to the premises should be controlled by methods appropriate to the particular situation. In some cases two control points will be appropriate:

Control Point 1 - would be the reception desk where a person is only allowed access if signed in and accompanied by an authorised member of staff, responsible for supervising the person while on the premises;

Control Point 2 - would be an electronic access system to a particularly sensitive or target area.

Asset Control and Records

In addition to property marking, it is recommended that the equipment be subject to the following asset control procedures:

- Maintenance of an inventory of all equipment including make, model, serial number, any distinguishing features and date of purchase. The record should be kept in a secure facility away from the equipment
- Registration of ownership with the manufacturer or a database
- Regular reviews of property identification to ensure records are up-to-date
- Equipment at a designated location to be the responsibility of a nominated person. Strict procedures to be enforced to prevent removal of or tampering with equipment without the authorisation of that person.

Data and Applications

To limit the disruption caused by loss of data and software applications, a procedure should be in operation to ensure that back-up copies are made together with any operating information and programme listings. Copies should be made at a frequency dependent on the value and nature of the data and software (as a general rule, data should be backed-up at least once every twenty-four hours) and it is recommended that verified back-up copies be kept in a data safe preferably at another location. Any safe keys and/or notes of combination numbers should be kept in the personal custody of authorised personnel and not left in the premises where the safe is located when unattended.

The copies should be subject to routine tests to ensure that if the need arises they will adequately replace the originals and systems will operate correctly.

Disruption to IT operations, and all activities of the organisation that rely upon these, can be further minimised by having detailed recovery plans including re-build and re-load manuals, which are regularly up-dated and exercised.

More information

The following two Risk Management Guides may also be useful when thinking about protecting your computers and other office equipment. Both are available now on the **MORE TH>N BUSINESS** website www.morethanbusiness.com

- New Alarm Installation Risk Management Guide
- Security Alarm Management Risk Management Guide

In Conclusion

Loss experience has demonstrated that this type of crime can only be deterred by an integrated package of measures, e.g. physical barriers, access control, intruder alarm protection, lockdown devices and permanent overt marking.

Risk assessments should be repeated at regular intervals, taking account of revisions to the inventory of equipment and changes in crime trends at both a national and local level, to ensure that any increase in the perceived threat or vulnerability is matched by a commensurate upgrade in security arrangements.

IMPORTANT

The information set out in this document constitutes a set of general guidelines and should not be construed or relied upon as specialist advice. Therefore **MORE TH>N BUSINESS** accepts no responsibility towards any person relying upon these Risk Management Guidelines nor accepts any liability whatsoever for the accuracy of data supplied by another party or the consequences of reliance upon it.