

## **INFORMATION SECURITY: PHYSICAL SECURITY CHECKLIST**

The following is a series of practical steps you can take to help preserve the security of your information and supporting systems.

Many of the actions are common sense (if they seem simplistic, they are!) and will also help your organisation in matters unrelated to information security.

- Survey your building(s) and deal with obvious problems. Put decent locks on your doors, install strong windows, and make sure people shut up shop at the end of the day. One tip is to seek advice from the local Crime Prevention Officer.
- Put servers and other vital specialist equipment in dedicated rooms with locked internal doors and no windows.
- Install appropriate air-conditioning and fire-detection systems in these special rooms.
- Avoid locating critical equipment near vents, pipes, kitchens, toilets, radiators and other similar hazards.
- Turn screens off at night (this prevents a tell-tale glow).
- Keep a list (or asset inventory) of all systems, memory, processors, serial numbers, locations and dates purchased.
- Put permanent labels on your valuable equipment. Perhaps try ultra-violet marking of equipment – this can help in recovering stolen items.
- Keep backups of your information well away from the source systems, and if possible off site.
- If you have multiple sites, spread computers across them (e.g. have separate domain controllers in different buildings).
- In shared, public or open areas (e.g. receptions) use Kensington (cable) locks to attach valuable equipment to desks.
- Minimise the amount of paper and sensitive information left on desks. Lock documents in cabinets (establishing a 'clear desk' policy if possible). This is not just for security: if there is a fire, the water used to control it can cause massive damage to paper, sometimes in excess of that caused by fire! Also, remember that even minor damage to a window on a windy day can cause loose paper to be blown around!
- If your company consists of more than about 15-20 people, issue visitor badges and encourage staff to challenge unaccompanied visitors.
- Escort all visitors – don't let them wander around unsupervised.
- Keep a visitor book and log the times when visitors enter and leave the premises. Keep another signing-in/-out list for sensitive areas, such as computer rooms.
- Consider CCTV in critical IT areas (e.g. server rooms) and reception areas.
- Get appropriate insurance, even if your business is a very small concern.

Please refer to the guidance on physical security in our business advice pages (see below) for further information.

### **Further help and advice**

#### **General**

BERR Information Security Health Check Tool  
<http://www.securityhealthcheck.berr.gov.uk/>

BERR Information Security Home page  
[www.berr.gov.uk/sectors/infosec](http://www.berr.gov.uk/sectors/infosec)

BERR Information Security Business Advice pages  
<http://www.berr.gov.uk/sectors/infosec/infosecadvice/page10059.html>

BERR Information Security Publications (available to order or download)  
<http://www.berr.gov.uk/sectors/infosec/infosecdownloads/page9935.html>