

Computer Security

Introduction

The expansion in the availability and use of computer equipment has been accompanied by an increase in crime in this area. The relatively high value and anonymity of the equipment attracts thieves, while the malicious interference of computer systems and the data they hold also appears to be on the rise.

Risk Assessment

The impact that computer equipment and systems crimes can have on your organization should be considered to enable you to identify cost effective security measures. Consideration should be given to:

- The nature of the premises, their location and the hours of occupancy.
- The effect that loss or damage to key equipment could have on your organization's ability to operate.
- The cost of replacing equipment and the waiting time involved.
- The most vulnerable areas of the premises in terms of thief access.

General Security Precautions

Implementing the following general security measures will help your organization combat computer related crime:

- Maintain an asset register of all equipment including their serial numbers and their location.
- Restrict equipment and systems access by using passwords and/or procedural controls with a clear audit trail in place.
- Install anti-virus software and internet firewalls.
- Advise users not to leave their equipment unattended without locking their workstation.

- Advise users not to leave equipment in unattended vehicles.
- Advise users to avoid carrying equipment in recognizable bags in public.
- Avoid sitting computer equipment near easily accessible windows.
- Do not advertise the arrival of new equipment by leaving its packaging outside.
- Backup important business data and keep copies off site.
- Produce a 'continuity plan', which will assist in getting computer systems back to normal after a security breach or loss.

Premises Security – Physical Measures

The level of physical security required will depend on the outcome of the risk assessment of burglary.

Security advice is available from your insurance company or police crime prevention officer but in general terms you should ensure that:

- Walls, roofs, windows and doors are of sound construction and good condition.
- Good quality locks and padlocks are fitted to windows and doors.

Installing either laminated glazing, steel shutters, gates, bars or grilles to windows and doors can offer additional protection.

IT and server rooms have a high concentration of expensive equipment. These rooms should therefore be robustly built and sited away from outside walls, ideally on an upper floor. Doors to these areas should be fitted with a good quality key operated lock or access control system.

Premises Security – Electronic Measures

The following electronic security measures can be a useful means of protecting your computer equipment from the risk of theft:

- **Intruder Alarms** – range from audible only systems to alarms that are monitored at ULC listed central station.
- **Smoke Generating Devices** – usually installed alongside an intruder alarm and work by very rapidly filling a protected area with a dense non-harmful smoke, which prevents the intruder from seeing the items they are trying to steal. These products leave no residual dusts or other contaminants in the area.
- **Remote Monitored CCTV** – pictures are sent to a CCTV monitoring centre enabling potential intruders to be detected and appropriate action taken. The cost of an effective system can be high.
- **On Site CCTV** – the images can be viewed during working hours enabling staff members to respond to suspicious activity.
- **Access Control Systems** – this system enables persons seeking access to the premises to be vetted and the movement of persons within the premises to be tracked.

Specific Equipment Security

Security measures applied specifically to pieces of equipment can further improve security. Options include:

- Permanent and visible marking of equipment with your name and postal code which will remove the anonymity of the equipment thereby reducing its attraction to thieves.
- Securing equipment in place with cable ties, which are a cheap and simple means of hindering rapid removal.
- Securing equipment with steel enclosures/entrapments that are bolted to the floor or desk.
- Securing 'dongles' (plug in keys that enable systems to operate encrypted/specially-licensed software) within a steel enclosure separate from the computer equipment. Therefore, if the equipment is stolen, the dongle should be left behind, thus avoiding the cost and inconvenience of having to buy new software.
- Equipment alarms can be installed which emit an audible signal if equipment is moved or interfered with.

- Equipment that is used in connection with the Internet can have software installed that sends a message if the computer is used from an unauthorized location. Similarly, certain companies offer to register your equipment and, should it be stolen and re-used on the Internet will detect its presence and notify you/the police of its reuse and current location.

Key Action Steps

- Complete a risk analysis to identify priorities.
- Review premises security with particular attention to the location and vulnerability of computer equipment. Do not rely solely on one or two measures – the most effective approaches usually involve the creation of a 'layered' security environment.
- Evaluate requirements for additional equipment protection (e.g., lockdown plates and alarm systems).
- Mark-up all equipment and maintain an up to date inventory.
- Review data and system security procedures.
- Re-evaluate Business Continuity/ Disaster Recovery Plan and ensure it is current and effective.
- If circumstances change, for example if new equipment is installed, a new risk assessment will need to be completed.
- If you do experience a criminal loss it is very important to take immediate steps to review and improve security to avoid becoming a 'repeat victim'. This term is used to refer to the well-documented problem where a theft is repeated in a short space of time.

Useful Contacts

Canadian Alarm and Security Association
National Office
610 Alden Road Suite 100
Markham ON L3R 9Z1
(905) 513-0622
Toll Free 1-800-538-9919

International Window Film Association
P.O. Box 3871
Martinsville, VA 24115-3871
Phone: 276-666-4932
www.iwfa.com