Loss Prevention Standards – Asset Classes

Computer Equipment Security

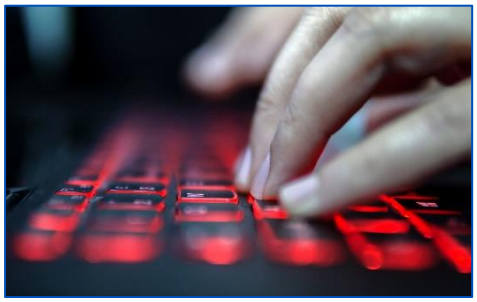
Version: 1.1
Date: 05th November 2024

Certain items of computer equipment are generally considered theft-attractive and are essential to the operations of most businesses. This document provides guidance to organisations on issues to consider when implementing security arrangements for this type of equipment.

AVIVA

Computer Equipment Security

Introduction



There are few if any commercial premises that do not have at least one computer and in most large organisations, computer equipment and their related communication's networks, are commonplace.

In the early days of widespread computer ownership and use, the theft of computers and their memory chips was a major problem. Nowadays, this seems to have reduced. However, in its place other malicious and criminal activities relating to computers has seemingly increased over time, such as hacking and data theft, etc.

When it comes to hardware, thieves can be attracted by the portability, value and general anonymity of many items of equipment, such as laptops and tablets. These are still 'popular' items for theft, as are high specification network or web servers. The latter being generally more attractive to organised or professional gangs, who can on occasion be prepared to use extreme force to obtain them.

With regard to software, hackers or disgruntled employees may view malicious interference with systems as a challenge, for a ransom, or be more attracted to the (criminal resale) value of personal information contained within them.

Note: Whilst this Loss Prevention Standard outlines some basic computer security measures, protection measures to prevent data theft or system interference is a very complex topic which is beyond the scope of this document. If you require further or more detailed support there are other resources available, such as the RISCAuthority publication *S28 – Cyber crime: overview and sources of support.* Alternatively consider obtaining specialist advice on this topic.

Risk Assessment

The necessity for all security, but in particular computer equipment security measures should always be determined after considering the impact on your organisation, via formal Security and Business Impact Risk Assessments, which should consider:

- Actual cost of replacing computer equipment, systems or data
- Expected equipment/software replacement times
- Vulnerability of premises, systems or data to unauthorised physical or electronic access
  - Ransomware or Malware
- The effect on your business operations
  - Direct and indirect business impact
  - Reputation and customer confidence

Computer equipment security measures can be considered under several broad headings, including: procedural, physical, electronic or item specific, all supported and underpinned by any wider security measures such as access control, intruder alarms, closed circuit television (CCTV), physical guarding; etc. The most effective, robust security protection is generally considered to be a joined-up approach adopting a range of complementary measures based on a formal risk assessment.

When reviewing computer equipment-related security measures, businesses should check whether any interested parties such as an insurer or a leasing company, has any specific requirements.

Procedural Security Measures

Options to consider include:

- Ensure access is limited to appropriately authorised individuals such as employees and customers and that access is:
  - Reviewed periodically
  - Removed when someone leaves the organisation or if procedures are not followed
- Passwords and other procedures should limit individual access to required systems and equipment only
- Install and maintain up-to-date anti-virus software and internet firewalls
- Implement strict and clear employee controls on use of the internet, downloading software, use of data encryption and memory sticks, etc.
- Ensure users are aware of the theft risks of leaving equipment unattended in public areas, sections of the workplace or when working away from the premises
- Ensure users don't leave equipment in unattended vehicles
- Ensure users don't travel with items such as laptops in easily recognisable carrying cases
- Do not position theft-attractive equipment next to externally accessible glazing
- Maintain an asset register, i.e. a list of all serial numbers and installed locations of computer equipment
- Avoid inadvertently advertising the arrival of new equipment, and do not:
  - Stockpile or store in readily visible locations
  - Leave in non-secure or common areas, etc.
- By way of a deterrent, it may be prudent to advertise any security measures that may not otherwise be readily apparent. As an example, post notices that the premises have a remote signalling intruder alarm system or that equipment marking systems are in use, etc.
- Ensure critical and important computer data is regularly backed-up and copies are maintained off site in a secure location
- Develop and maintain a Business Continuity Plan (BCP) to support the recovery of your computer systems after any security (or other) incident. This should be:
  - Maintained up to date, reviewed and revised periodically
  - Tested regularly

Physical Security Measures

Premises

A well-secured perimeter, either to the building in its entirety or to specific areas within the premises (ideally both), will provide major benefits. Perimeter protection should take account of the:

- Nature of the buildings
- Location
- Ease of access
- Hours of occupancy
- Type (theft-attraction) of the computer equipment present within

IT suites and server rooms in particular, often contain concentrations of expensive or critical equipment. Organisations should ensure these are robustly built, sited away from outside walls (ideally on upper floors), not visible from outside of the building and that good quality doors and locks are fitted.

Guarding

At some premises the values at risk, the business exposure or the effect of a loss to reputation should an incident occur, etc., may require a physical guarding presence, during or outside business hours, or both.

The National Security Inspectorate (NSI) listing is an indicator of full compliance (supported by external auditing) with UK manned guard licensing rules and good security practice, e.g. adherence to recognised British Standards.

Membership of the Security Industry Authority (SIA) Approved Contractor Scheme (ACS) is also indicative of good standards.

Although it may conflict with operational convenience, care should be taken to ensure that guards are suitably protected against duress, i.e. they cannot be forced to unset alarms or unlock doors, etc. This is best completed by stationing guards outside of any building they are guarding and not permitting them to hold keys, codes or un-setting devices for electronic security systems.

Electronic Security Measures

If the items of computer equipment within a building are of sufficient theft-attraction, thieves will often go to the trouble of overcoming physical security measures. In such circumstances, electronic security devices can effectively supplement physical and procedural measures, with options including the installation of:

- An access control system to assist in vetting/controlling persons seeking access to, or within key parts of, the premises
- A locally or remotely monitored intruder and hold-up alarm system. Additional guidance is provided in the Aviva Loss Prevention Standard: *Security - Intruder Alarms: Guidance for Customers*
- A locally monitored CCTV system to allow individuals to manage, monitor and/or record visitors during operational hours
- An external remotely monitored, detector-activated CCTV system. These can be particularly effective outside business hours in detecting potential intruders whilst they are still outside the premises, i.e. before a break-in is attempted or occurs. The nature of such systems requires careful attention to system design and operating procedures if they are to be effective. Additional guidance is provided in the Aviva Loss Prevention Standard: *Security – An Introduction to Closed Circuit Television (CCTV) Systems*
- A 'smoke' generating security fog device operated by alarm sensors. When activated, these rapidly fill an area with a dense, non-harmful chemical fog which obscures vision, and may prevent potential intruders from clearly seeing theft-attractive items whilst hindering their movement within the premises. Additional information on this topic is provided by the RISCAuthority via their publication: *S7 – Security Guidance for Fog Devices*
- A forensic intruder marking system. When activated, these fill an area with a near invisible, non-harmful, uniquely formulated chemical mist, which adheres to the clothes and body of intruders. The police can detect this marking on individuals and trace it back to the registered premises

Equipment Security Measures

Good site-wide procedural, physical and electronic security measures can provide a robust line of defence, but security measures applied to specific items of equipment can provide effective additional security and may provide an effective deterrent to potential thieves.

Options to consider include the following:

- Provide permanent visible marking (etching) of equipment with details of the company name and postcode
- Provide covert forensic marking
- Secure equipment to walls or furniture with steel cable ties to hinder removal - anything to act as a deterrent or to slow down and restrict the progress of thieves
- Secure equipment in an 'entrapment' device bolted/anchored to a floor, wall or desk. This will help prevent easy removal of the equipment or any internal components. Further guidance is provided in the Loss Prevention Certification Board Standard LPS 1214 Issue 2.2 *Specification for testing and classifying physical protection devices for personal computers and similar equipment*
- Use of secure plug-in dongles (devices that enable or encrypt software to specific users or computers) within a steel enclosure separate from the computer equipment, e.g. under the desk. If the computer is stolen, the dongle should be left behind, avoiding the need to buy new software and the inconvenience of not being able to run any back-up copies on replacement equipment
- Use of equipment alarms which emit an audible signal if the equipment is moved or interfered with. These are ideal for alerting nearby individuals to 'walk-in' theft or unauthorised use
- Use of internet tracing devices which can send a message if a computer is used from an unauthorised location, e.g. after being stolen, which in turn can help establish its current location

Checklist

A generic Computer Equipment Checklist is presented in Appendix 1 which can be tailored to your own organisation.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- For information on CCTV, intruder alarms and physical guarding providers:
  Security Systems and Alarms Inspection Board (SSAIB)
- For general information:
  British Security Industry Association (BSIA)

  Master Locksmith Association

  RISCAuthority – Basic cyber security controls for the small business – awareness checklist

Additional Information

Relevant Loss Prevention Standards include:

- Intruder Alarms European Standard
- 12 Top Tips to Protect Against Cyber Attack
- Cyber Essentials Accreditation
- Cyber - Social Engineering
- Business Impact Analysis
- Business Continuity Management
- Business Continuity Plan – Testing and Maintenance
- Managing Change - Property

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*Calls may be recorded and/or monitored for our joint protection.

Appendix 1 – Computer Equipment Security Checklist

Location	
Date	
Completed by (name and signature)	

	Computer Equipment Security	Y/N	Comments

1.	Have Business Impact and Security Risk Assessments been undertaken of the current IT/computer security at your premises, including the following?
	• Local or business history of IT security related events?
	• The cost of replacing computer equipment, systems or data?
	• Expected equipment/software replacement times?
	• Accessibility and vulnerability of premises, systems or data to unauthorised physical or electronic access?
	• The business impact on your operations:
	  ○ Reputation and customer confidence?
	  ○ Loss of computer equipment, systems or data?
	  ○ Malicious interference with computer equipment, systems or data?
	• Strength and nature of the building construction, doors, windows and securing mechanisms?
	• The nature of any other electronic security measures or human presence on site?		

2.	Has any independent or specific crime prevention advice or security requirements been sort from: • The Police? • A security consultant? • Your insurer? • Equipment leasing company?		

	Computer Equipment Security Contd.	Y/N	Comments
3.	Do your password rules and other procedures limit employee and customer access to systems and equipment?		
4.	Has anti-virus software been installed and is this up to date?		
5.	Are there clear employee controls on internet usage, downloading software and the use of data encryption?		
6.	Have users been made aware of the theft risks of leaving equipment unattended in public; in unattended vehicles; carrying items in recognisable laptop bags; leaving them in clear line of sight of windows and doors?		
7.	Is an asset register maintained of all serial numbers and the location within the business of computer equipment?		
8.	Is important and critical computer data regularly backed-up? Are copies maintained securely off site or in a different building at least 30m away?		
9.	Has a BCP for the IT hardware and systems been prepared? • Is this a live document which is regularly reviewed? • Is this tested?		

10.	Has the location of any IT or server rooms been considered?
	• Are these visible or accessible from the building exterior?
	  ○ Are additional measures in place to protect any glazing to the exterior?
	• Can the room be accessed through a weak vulnerable ceiling/floor above or from a floor below?
	• Is access to these areas restricted the closer one gets to the room?
	• Are these rooms locked at all times?
	• To prevent 'unmanaged open doors', do the doors into the room have automatic closing and latching mechanisms?
	  ○ Are door wedges prohibited?
	• Is access to these rooms limited to a named group of individuals?		

	Computer Equipment Security Contd.	Y/N	Comments
11.	Are the premises protected by electronic security systems? • A CCTV system? • An access control system? • A remotely monitored intruder alarm system?		
12.	Is the computer equipment hardware 'property-marked'? • Visible marking (etching) of equipment with details of the company name and postcode? • Covert forensic marking?		
13.	Is high value or business critical equipment secured by a proprietary 'entrapment' device? Is this bolted/anchored to a floor, wall or desk to prevent easy removal of equipment or internal components?		
14.	Are secure plug-in dongles (devices that enable or encrypt software to specific users or computers) used for critical systems or operators?		

15.	Are the security measures of the IT hardware equipment and software systems considered within a formal Management of Change process?
	• For new software systems?
	• For new hardware?
	  ○ Delivery?
	  ○ Receipt?
	  ○ Storage?
	• For removal of old hardware?
	• New employees?
	• Departing employees?		

16.	Are all employees formally trained on your IT policies and security measures, and does this include: • All employees? • Contractors? • Repeat training?		

	Computer Equipment Security Contd.	Y/N	Comments
17.	Are security arrangements and the basis for the risk assessment reviewed following any security issues, local incidents, intrusions or losses etc.? Note: If not, you are likely to be at more risk of a repeat incident.		
18.	Additional comments:		

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

05th November 2024

Version 1.1

ARMSGI1422020

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

LOSS PREVENTION STANDARDS