AdviSec Ltd

Physical security

Aims

For ‘hundreds of years’ groups, businesses, Government departments and nations have implemented physical security measures to counter the threat from hostile attackers. Today the technology may have changed, but the threats remain, and no one can doubt this fact.

Advisec Ltd through its CLAS (CESG Advisor Scheme) and CISSP (Certified Information Systems Security Professional) consultants, specialises in providing advice on physical security matters, specifically best practise approaches such as defence-in-depth to organisations and associated affiliations, for example building companies / architects (for ‘new’ build) and property services departments.

Consideration of Business and Technology Issues

Threats include:

- Terrorist attacks
- Groups seeking information for personal gain (e.g. journalists)
- Theft
- ‘Acts of God’ (e.g. flooding)
- Power failure.

Physical security measures:

- Perimeter defences, e.g. Fences/walls, Barriers / bollards, Intruder detection systems (alarm system), surveillance/CCTV, Patrols, Lighting
- Entry control systems, e.g. swipe/proximity card access systems (ACS), fingerprint / IRIS scanners, Reception areas
- Accounting measures, e.g. CCTV recorder, logs from ACS
- Environmental controls, e.g. air conditioning, UPS / generators, Smoke alarms & fire suppression equipment.
- Vigilance of staff
- Secure furniture, e.g. cabinets

Also for consideration:

- The convergence towards IP offers the opportunity to share infrastructure (thereby reducing costs), for example CCTV over IP

- The convergence towards IP offers the opportunity to manage components from a single platform, e.g. locking and unlocking doors, intruder and environmental alarms, and lighting.
- Are there opportunities to reduce the dependence on 'traditional' security measures in favour of cheaper IT-security measures?
- Minimise the risk by ensuring that physical security measures, operating procedures and IT controls are aligned.

Client Engagement

Phase 1

Conduct a survey of the surrounding area from a 3-D perspective to gain an appreciation of the 'threat' environment.

Liaise with representatives from the client organisation to determine the purpose of the building / site, and the requirements and provision for access:

- Data centres / control rooms(?)
- People, e.g. Staff groups, Contractors and other third parties, maintenance and ancillary staffs, and suppliers
- Utility supplies (e.g. power, water)

Identify the assets to be protected, and the level of protection required. Note the afforded level of protection for such assets could either be marked in accordance with an organisational policy, or alternatively Advisec would undertake such an exercise using the UK Governments security marking scheme.

Liaise with the client organisation, and conduct a survey to ascertain what physical security measures are in-place.

Phase 2

Undertake a gap analysis for each asset (or group of assets) by methodically assessing the risk associated with each threat and potential means of compromise (or 'entry points')

Recommend security measures that:

- Address the security risks (mitigating the risk to an acceptable level)
- Reflect the convergence towards IP
- Result in a cost effective solution

Phase 3

Procurement and Implementation phase.

Phase 4

Conduct inspections and intruder testing to confirm that the physical security measures are operating effectively. Note this activity can be a 'sensitive' activity and needs careful planning.

Benefits to Clients

The client organisation can be assured of high quality security advice provided by security accredited consultants i.e. CLAS and CISSP, and based on the experience and knowledge accrued in earlier engagements with clients, including UK Police Force and UK MOD.

Contact us:
Further details, including case studies, presentations and references are available from Nigel Strutt. Please call 01869 388011 or 07780 526195. Head office; 41, Barry Avenue, Bicester, Oxfordshire. OX26 2DZ. Email: nigel.strutt@advisec.co.uk