Site Security & Certification

We have a belief that security must be viewed holistically, which is why we realise that meaningful and cost-effective physical security measures can be overlooked at the expense of technical security solutions. In today's climate, no organisation should think twice about protecting its information assets through the use of logical measures, such as a firewall or Intruder Detection System (IDS) at the perimeter - and the same must be applied in the physical realm.

Look to the bigger picture before committing

Before building your fortress, the first thing you need to consider is the value of your asset. It's also necessary to weigh-up threats, the likely attackers and their compromise methods. How far in the sand do you need to dig your penny before you can be sure that even the most desperate of thieves will not try to steal it? In combination with the asset value and threat, any vulnerability is also a necessary consideration – for example, if the thief saw you dig your penny in they will know where to start once you depart. Although, if your penny was actually a briefcase full of £100 notes, you would be likely to take an instinctive risk-management decision to secure it somewhere more conventional like a bank; the same can be said for your information assets.

Physical Security the Layered Approach

As with the combination of all aspects of security, physical security requires a layered approach – the 'onion skin approach'. For ease of interpretation physical security layers, working from the outside in, can include the following:

- **Perimeter**: such as external fences and walls to offer a level of delay to forcible attack.

- **CCTV**: with varying degrees of presence, siting and scrutiny; from dummy cameras, which act only as a preventative measure; to out-of-hours, or 24x7 monitoring by local or remote professional response teams; interconnection of CCTV with other Permimeter Intrusion Detection Systems (PIDS) for enhancement of complimentary security systems where a

breach is sensed; through to recording of CCTV-captured events for facial recognition to act as evidence in criminal proceedings by the courts. Of course, as an organisation or business you will need to justify an appropriate degree of CCTV technology and will be expected to conform with the CCTV Code of Practice and the Data Protection Act.

- **Intruder Systems**: which includes PIDS; sensors and electrified fences, etc.

- **Guard Service**: well organised static and patrolling uniformed guards provide a deterrent to criminal and terrorist activity.

- **Building, Area or Site Entry Controls**: fences, walls, barriers and access-control equipment and systems. For example, an automated access control system for personnel, or access barrier, which deters/prevents access to vehicles.

- **Building Construction**, which could be anything ranging from a lightweight structure resistant to weather only, to a building designed to resist a substantial forced attack from a capable group with specific tools.

- **Rooms** which can range from a standard locked office, secure conference and telephone rooms (for prevention from eavesdropping) to lightweight secure rooms, and strong rooms without windows and of specific attack-resistant construction.

Locks can range from those used to secure doors and windows, to those used secure containers; these can range from privacy only through to approved security rated locks (i.e., self-powered electronic combination locks, electronic combination scroll locks, or manifoil combination locks).

Containers, such as portable security boxes, cupboards and filing cabinets, and computer hardware containers; equipped with a range of privacy or security rated locks.

Other factors for consideration are:

- **Receipt, Registration & Recording** of sensitive assets and hard copy documents.

- **Handling & Movement**; does your equipment or documents require secure packaging in transit; should tampering be prevented, should packages be carried by specific or multiple personnel; would you entrust a package of this nature to a postal service, and if so what standard of delivery would you expect.

- **Destruction & Disposal, or Re-Use**; once an item of equipment (for example a laptop or printer) has come to the end of its lifecycle you need to consider disposal; would you throw it away with general waste, or would you require professional destruction. Or could the item be re-used elsewhere in your business, or could you sell it – in either case you would need to consider the value of the data held in the device memory and if it could be easily recovered.

Site Certification

If you are a commercial organisation planning to hold and secure protectively marked information on behalf of a Government client – predominantly Ministry of Defence (MoD), your site(s)[1] will be expected to meet a specific score in a physical security assessment (Security Assessment for Protectively Marked Assets (SAPMA)); in addition you will be expected to augment physical security with demonstrable procedural and personnel controls. By appropriately preparing, and successfully demonstrating (through external assessment) an ability to maintain your security posture, your site should achieve 'List X' certification.

Where your site is involved in the business of security of Sensitive Nuclear Information (SNI), you must achieve accreditation against 'List N' criteria. 'List N' sites may be further categorised as 'Type A' or 'Type B' sites depending upon such factors as type of establishment or the amount of SNI held or processed on site.

[1] If you intend to hold protectively marked Government information at multiple sites, each site must be certified in its own right.

The 'List' naming principle is based on the fact that the relevant authority (Principal Security Advisor (PSyA) for Defence Equipment & Support (DE&S) (MoD) or the Information Security Branch of the Office for Nuclear Regulation (ONR)) has access to a controlled and protectively marked RESTRICTED 'list' of sites that have achieved the relevant accreditation standards.

Similarly, if your organisation conducts business on behalf of the Government Communications Headquarters (GCHQ) or CESG (the National Technical Authority for Information Assurance) you will need to conform to its own physical security inspection criteria.

Depending upon your holistic security stature and the threat to your organisation, by location or profession, you may be somewhat bound by the specific types of security standards you apply.

Your site will not be certified solely on the basis of a 16ft impenetrable perimeter - you will need to score sufficient points in all of the areas discussed here (some of which have minimum mandatory scores). Of course if you do have a strong perimeter, access controls and supporting personnel controls, then a lack of points in other areas may be risk-managed.

Although physical security has been the main aim of this document, it must be noted that physical security is unlikely to have the full anticipated effect if not appropriately overlapped by other procedural, technical or personnel security aspects. For example, if the people you employ to process your sensitive information and lock it away in your heavy steel safe with Mark 4 manifoil lock are foreign nationals with no character or professional references, then you may have wasted the best part of £1100 on a cabinet to store your documents.

Regency

Whether an organisation is looking to reduce their risk profile by including physical security within the design and planning phase of a new installation, or to augment or upgrade existing security measures, we have the experience, knowledge and capability to provide value-added risk reduction and mitigation advice - from the initial site survey through to solution implementation and on to review and audit - all of which are designed to enhance your operational capability (and potentially that of your business partners) rather than limit it. Physical security audits tailored to any security standard are also familiar ground for our consultants.

Regency consultants draw on our up-to-date knowledge of, amongst others, consultants with good physical security knowledge from military backgrounds, the Security Policy Framework (SPF), the Centre for the Protection of the National Infrastructure (CPNI), its Catalogue of Security Equipment (CSE) with equipment approved by the Security Equipment Assessment Panel (SEAP), Sensitive Information Compartments and Industry Standards.

Regency also have experience in training staff, including Police Officers, in physical security, allowing them to carry out their own surveys and producing reports for management.

At Regency we practice what we preach, we currently maintain our own certifications against all three Authorities discussed in this paper. As such we fully understand how to tailor the security requirements of facilities either merely seeking a higher level of security, or certification against any security standard.