Physical Security & List X

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.

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 inside out, can include the following:

- **Containers & Locks**, such as portable security boxes, cupboards and filing cabinets, and computer hardware containers.

- **Rooms & Locks**, which can range from any locked room, to a strong room without windows and of specific attack-resistant construction.

- **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.

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

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

- **Intruder Systems**, which includes Perimeter Intruder Detection Systems (PIDS); sensors and electrified fences, etc.

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

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 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.

List X

If you are a commercial organisation planning to secure protectively marked information on behalf of a Government client, you'll be expected to match or exceed a specific score in a physical security assessment (Security Assessment for Protectively Marked Assets (SAPMA)).

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. You will not be List X accredited solely on the basis of a 16ft impenetrable perimeter - you will need to score sufficient points in all of the areas discussed here. Of course if you do have a strong perimeter, the points required in other areas are likely to decrease respectively.

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 IT Consulting

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 the clients' operational capability rather than limit it. Physical security audits tailored to any security standard are also familiar ground for our Consultants.

Regency IT Consultants draw on our up-to-date knowledge of, amongst others, Consultants with good physical security knowledge from military backgrounds, The Centre for the Protection of the National Infrastructure (CPNI), the Security Policy Framework (SPF), the Catalogue of Security Equipment (CSE), STRAP 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.

Regency List X

Regency IT Consulting operate from a List X facility (formally approved to store and process Government Protectively Marked information), where we currently and continually conduct business on behalf of many Government clients. In addition, we have a number of information systems, for which we hold ISO/IEC 27001 Certification.

IS 548043

At Regency IT Consulting we practice what we preach and fully understand how to tailor the security requirements of facilities either merely seeking a higher level of security, or those seeking certification against any security standard.