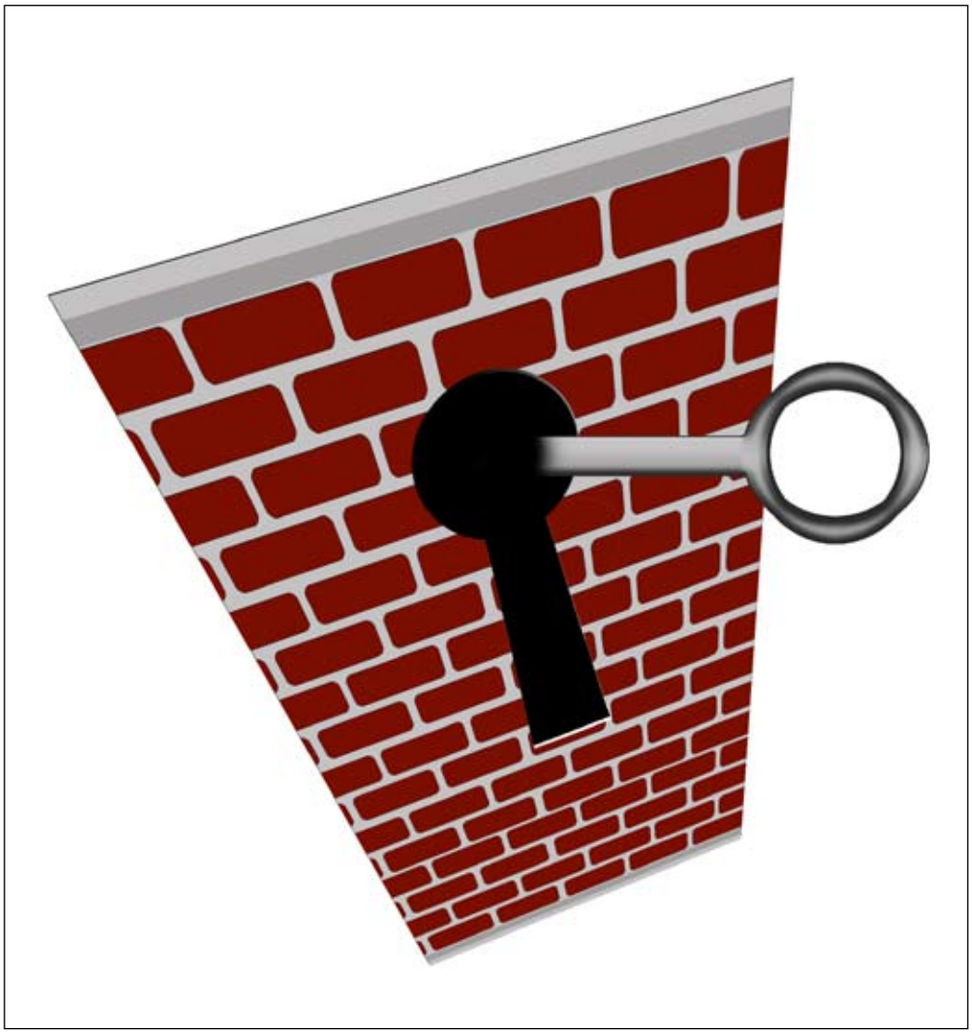
Creating Barriers Is Good For Business

Layered Security – *Physical & Procedural Security*

Simarjit Chhabra, CIO, Xtralis



Shocked? You shouldn't be. Read on - you will be able to understand why it's important for any business to design and implement a layered defensive security model to protect people, information or critical resources, including Intellectual Property.

It is commonly accepted that the greatest potential source of threats to systems is 'the insider': staff, contractors and anyone else who has logical or physical access to the system. It is also commonly accepted that the majority of security breaches caused by insiders are not malicious but the result of ignorance i.e. a lack of training or awareness or vulnerabilities arising from inadequate physical security or lapsed working procedures.

The increasing trend for businesses to utilise the virtual workforce and mobile computing diminishes control over the physical environment and makes the need for procedural security more important then ever before. Experience shows that staff who do not appreciate the need for procedures will sooner or later find ways around them. In order to ensure staff honour their security obligations, it may be necessary to carry out security education, training and awareness to promote the concept that everyone in the organization has a responsibility to address physical and procedural aspects of information security in their daily work.

> The greatest potential source of threats to systems is 'the insider'.

Before we dive into details, let's understand the threats and vulnerabilities which face the business.

Threats and Vulnerabilities
The primary goal of physical, environmental and procedural security is to ensure that the system is available when needed and maintains data integrity and the confidentiality of the information it manages. This is known within security circles as a CIA triad – Confidentiality, Integrity and Availability of information.

The physical and procedural threats to systems include both malicious and accidental actions, plus environmental conditions that may damage computer system hardware and media. The physical components of systems are at risk during installation, and when building maintenance or geographic relocation is under way.

Mobile systems including laptops, mobile phones, and personal digital assistants (PDAs) are particularly at risk in public transit and when left unattended in 'foreign' environments, such as hotel rooms.

The threats to the physical environment can be grouped into the following types of events:

Natural/environmental:
Earthquakes, floods, storms (i.e., thunder, hail, lightning, electrical, snow, and ice), tornadoes, hurricanes, volcanic eruptions, natural fires, extreme temperatures, high humidity, building collapse.

Utility/Supply:
systems Communication outages, power distribution (i.e., blackouts, brownouts, surges, spikes), burst pipes.

Man-made :
Explosions, disgruntled employees, unauthorized access (i.e.,hackers, crackers), employee errors, arson/fires, sabotage, hazardous/toxic spills, chemical contamination, malicious code, vandalism and theft, fraud and embezzlement, intruders, unintentional acts (i.e., spilled drinks, overloaded electrical outlets).

Political events:
Bombings, terrorist attacks, espionage, riots or civil disturbances, strikes.

It is commonly accepted that around 75% of all attacks perpetrated by insiders are in fact simply accidents or the consequence of ignorance of security obligations or lack of knowledge to operate the system securely. These can range from simply spilling coffee on the keyboard to the contractors cutting through the cable during site work. Experience has shown that many potential accidental threats can be avoided by education and good procedural security measures.

An external threat may also interrupt the normal operations of the systems. The extent of the losses depends on the duration and timing of the service interruptions and the characteristics of the operations performed by end users. Even simple damage to equipment — whether intentional or unintentional — can interrupt normal business operations, e.g. cause data corruption and increase cost of doing business as a result new equipment purchase. Most malicious threats disrupt business for longer than it may first seem, as it's rarely a simple matter of replacing hardware or restoring data from backup.

A physical attack may be targeted on the building or site, therefore damage to the infrastructure may need to be repaired before the computer system can be restored. Arson may entail recovering from the wider effects of smoke and water damage.

It is difficult to generalise on the possible sources of such attacks, but the information security professional should consider the capability, opportunities, and motivation of, for example, any relevant political or other pressure groups, competitors, and even former employees.

While planning for physical security, it is helpful to perform a risk analysis that focuses on existing threats to the computing resources and determines where countermeasures can be most cost-effective. It is important to consider all potential threats that represent an exposure, even the unlikely ones. When considering physical security, it is important not to cause conflict with life safety goals.

Life safety focuses on providing a safe exit from a facility under dangerous conditions. Life safety concerns will always override other security issues; however, it is possible to achieve an effective balance between the two goals. The most newsworthy cases have been those where organisations barred exits to prevent employees from opening the doors. In several tragic instances, a fire occurred inside a building and locked doors prevented employees from exiting the building, thus causing unnecessary deaths. Because of these incidents, several countries have implemented fire-safety regulations that ensure adequate exit points from buildings. A common example is installing emergency exit doors with a time delay. When the panic bar is depressed, a loud alarm sounds and the door is released after a brief delay. This allows time for a security guard to assess the situation.

Finally, information itself has a value: commercial plans, research and development data, staff directories, and other such information are of use to competitors, investigative journalists, hackers, and others. Many technical hacking attacks begin with information gathering and social engineering, for example, the collection of paper waste that has not been shredded or otherwise rendered unusable. As we plan for risk mitigation against the potential threats, we should also plan for the vulnerabilities which arise from inadequate or lapsed security working practises and weak physical security measures.

Site Location and Infrastructure

The location of the site has implications on the need for physical security for the system. An out-of-town location may provide complete control of the outermost perimeter by means of fencing, guard patrols, closed-circuit television (CCTV), and other intrusion sensors. In an urban area, however, that perimeter area may be as shallow as the building's walls or the floors the organisation occupies.

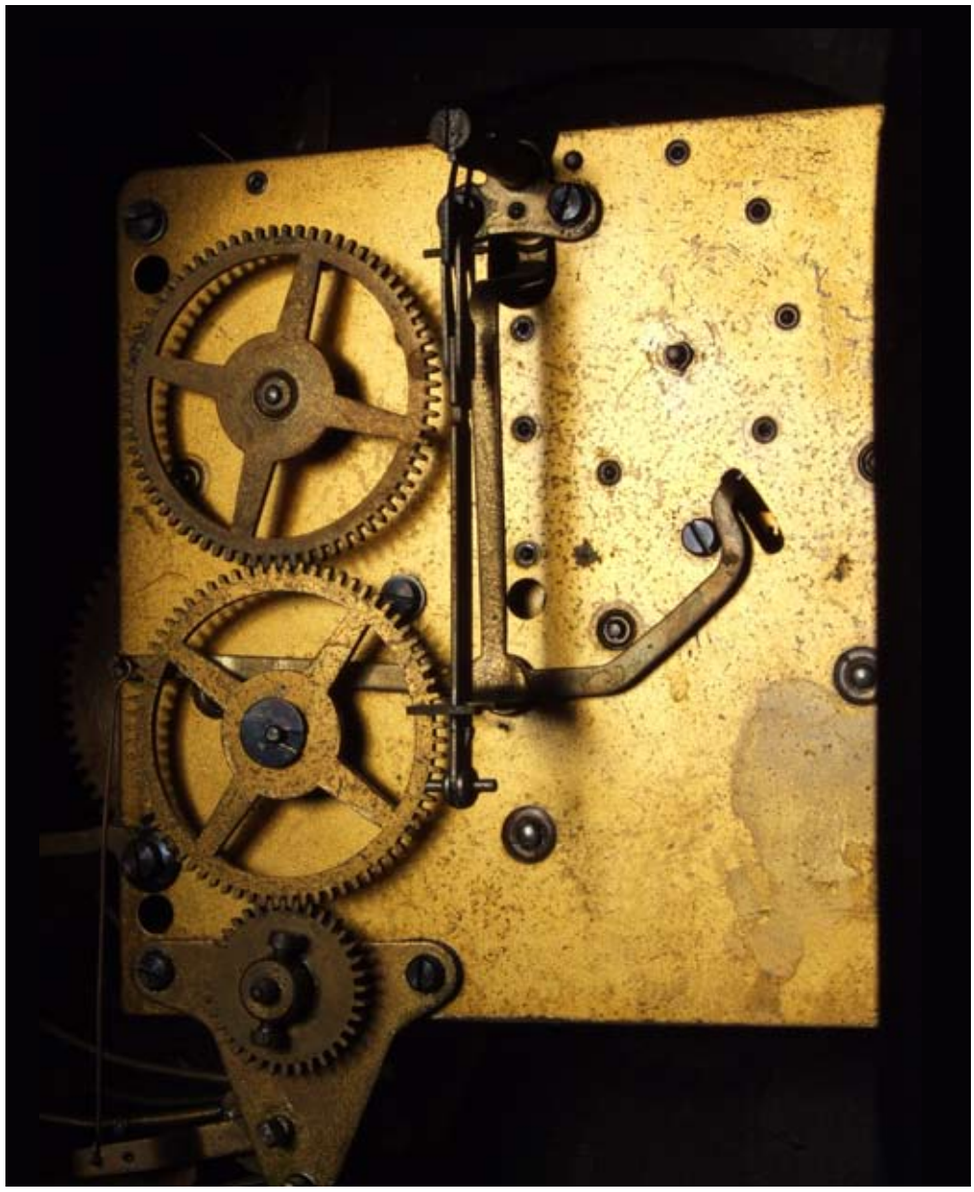
Where the organisation leases part of a shared building, control over external security may be difficult to achieve; although it can protect its own perimeters within the building, the organisation may not be able to legislate against attacks on the building itself, nor any shared infrastructure services, such as telecommunications.

The geographical location of the site may affect the security requirement if it is vulnerable to natural disasters, such as lying in a flood plain, is vulnerable to burglary, vandalism, street crime, and arson, or lacks adequate access for the logistical support of emergency services.

The layout of and materials used in buildings have implications on security, as does the provision of infrastructure - water, light, heat and ventilation, and power systems. In this area, security arrangements must comply with statutory health and safety requirements.

In modern buildings, it may be possible to change the layout to accommodate security requirements, for example, to place cabling in secure ducting under floors or in ceiling cavities. In older buildings, particularly where these are subject to conservation orders, this may be impossible and security must be addressed within given architectural constraints.

> “75% of all attacks by insiders are simply accidents.”



> The location of the site has implications on the need for physical security.

When a new site is built, or the organisation relocates to modern premises, there is an opportunity to influence infrastructure and physical security arrangements to best protect the systems. To achieve this, security will need to be considered at all stages of design and build.

The Layered Defence Model

The main aim of physical and procedural security should be to integrate with technical system security measures in providing defence in depth. This is defined as 'a layered combination of complementary counter-measures' or the layered defence model.

The number and nature of defensive layers will depend on the configurations of the sites in which the system is managed. Typically, they will include the outermost physical perimeter, inner perimeters, and security zones specific to the system.

The outermost perimeter is the furthest physical extent that the organisation can control; the innermost perimeter describes areas within this perimeter. Areas within the innermost perimeter, such as individual rooms or suites, require additional layers of protection.

In an open or rural environment, the outermost perimeter may comprise the fences, landscaping, and parking areas surrounding the buildings of the site. Inner perimeters may comprise individual buildings within this overall perimeter, and security zones may be needed for server rooms and specific data processing areas.

In an urban environment, the outermost perimeter may comprise the building or a suite of floors in a shared building that belong to the organisation. Inner perimeters may comprise specific floors or suites of rooms, and security zones may again comprise those rooms that specifically house the system itself.

These inner perimeters logically extend to communication systems and ducting that carries wire or fibre-optic cables between secure zones. While considering security for communications, it is important to note that physical security measures cannot protect wireless communication unless shielding measures are implemented to protect from the unintended emission and interception of signals from system components.

Every facility should have a reception area that is accessed directly from the public access zone. This ensures that visitors and maintenance personnel cannot proceed to an operational or secure zone without escorted access. If this process cannot be accommodated, then securing each floor should be considered. Whether each floor must be secured depends on the sensitivity of the information and costs versus the security alternatives.

Let's look at an example:

• A fence protects the perimeter.
– Vulnerability: unlocked gate
– Attack: the intruder enters through an unlocked gate at closing time.

• The building entry points are protected with a card access control system.
– *Vulnerability: cleaning crew has badge cards for access but are not trained in security practices*
– *Attack: intruder enters the building by 'tailgating' the cleaning crew; the cleaning crew does not stop or question the individual.*

• Inside the building, a card access control system protects the elevators and door locks secure the stairwells.
– *Vulnerability: to avoid waiting for the elevator or to sneak a cigarette in the stairwell, employees prop open the stairwell doors*
– *Attack: intruder enters through unlocked stairwell.*

• The office doors are also secured with locks.
– *Vulnerability: door is pushed shut but employee does not ensure that it actually clicked shut all the way.*
– *Attack: intruder easily pushes the door open (at this point, the intruder has managed to defeat the security control and gain access to an employee's office).*

• Inside the office, the employee has locked all sensitive information in an office safe.
– *Vulnerability: employee did not put all information in the safe or did not close the safe properly*
– *Attack: although information was left out of the safe, its content was not sensitive. (The employee did practice good security by putting all sensitive information in the safe and properly closing the safe. Unfortunately for the intruder, the safe has a high security combination lock that cannot be easily circumvented. Intruder was not successful!)*

This is the concept of a layered defence: if the intruder can bypass one layer of controls, the next layer of controls should provide additional deterrence or detection capabilities.

Another key element is using multiple types of security controls within each of the layers. For example, if the same key is used to unlock the front door, the elevator, and the office suite, the layered defence is minimised or neutralised because an intruder only has to subvert one layer: gaining access to the front door key. However using several types of controls, such as augmenting the locked front door with a surveillance system, can increase the ability to prevent, detect, or deter the event.

Several specific security technologies and tools provide physical protection controls which follow the layering model (i.e., perimeter to office suite) and outline the controls that can be implemented at each layer. Some controls can be implemented at various levels. For example, locks are used for both building entry points and office suite entry points. Layered security needs to be planned for each sublevel i.e.

> "The aim of physical and procedural security is to integrate with technical system security."

• Perimeter and building grounds
• Building entry points
• Inside the building: building floors, office suites, and offices.

Let's discuss how we can prevent crime by designing the environment to protect the system or the core resources.

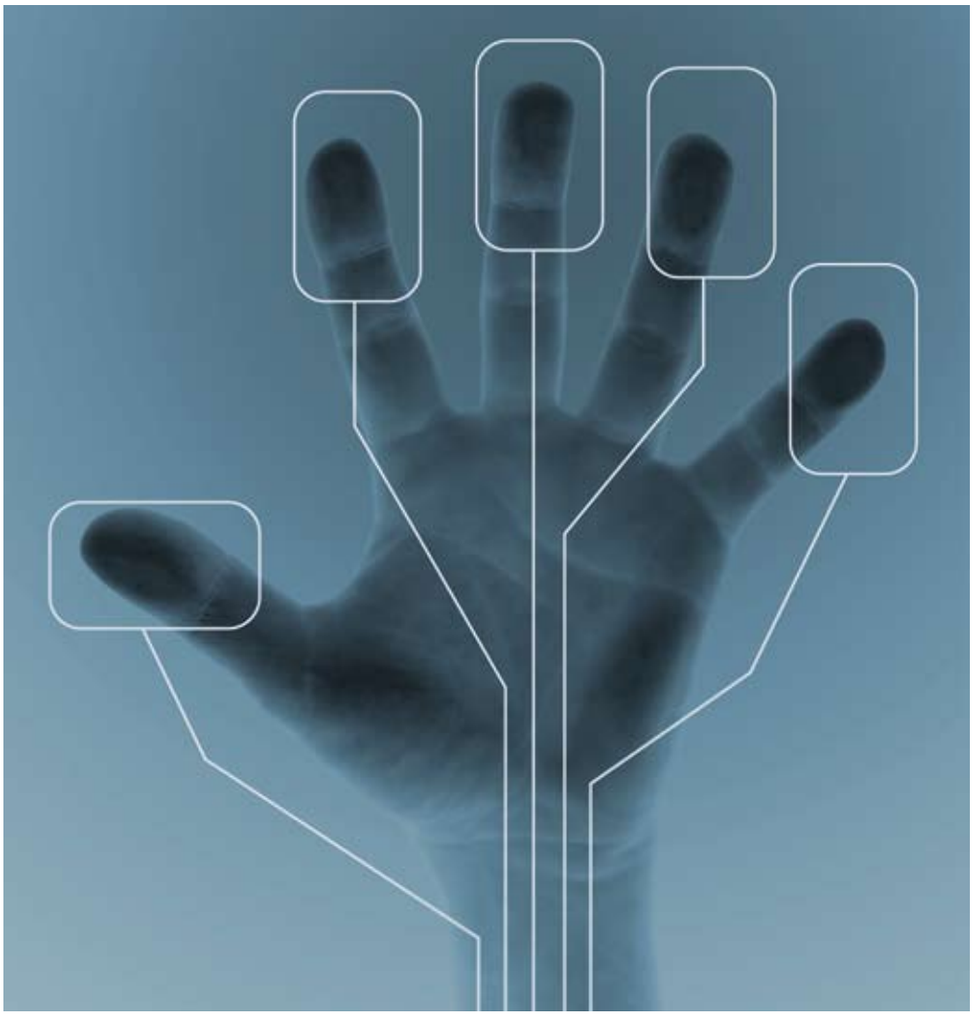
Crime Prevention through Environmental Design (CPTED)
Crime Prevention through Environmental Design (CPTED) is a concept that states that, as its basic premise, the physical environment of a building can be changed or managed to produce behavioural effects that will reduce the incidence and fear of crime.

CPTED is a branch of situational crime prevention that aims to reduce the opportunity for specific crimes or incidents to occur. By combining security hardware, psychology, and site design, a physical environment can be created that would, by its very nature, discourage crime. The focus on the relationships between the social behaviour of people and their environment is the essence of the CPTED concept. It contains elements that make legitimate users of a space feel safe and make illegal users feel unsafe in pursuing undesirable behaviour. For example, outside lighting may make employees feel safe, but may also provide deterrence to intruders.

CPTED builds on several key strategies: territoriality, natural surveillance, and access control. It's based on the psychological and sociological method of looking at security and describes how the physical environment might impact the security of an area or building.

Territoriality:
People protect territory that they feel is their own and have a certain respect for the territory of others. CPTED encourages the use of physical attributes that express ownership, such as fences, pavement treatments, art, signs, good maintenance, and landscaping. Identifying intruders is much easier in a well-defined space.

Surveillance:
Intruders do not want to be seen. Surveillance is a principal tool in the protection of a space. Environments where occupants can exercise a high degree of visual control increase the likelihood of criminal acts being observed and reported. Implementing physical features, conducting activities, and locating people in ways that maximise the ability to see what is going on discourages crime. For example, landscaping and lighting can be planned to promote natural surveillance from inside a building and from the outside by people passing by. Formal surveillance, such as closed circuit television (CCTV) or organised security patrols, is often used as an additional deterrent.



> Physical and procedural security are integral parts of information security.

Access control:
Properly located entrances, exits, fencing, and landscaping can control the flow or limit access to both foot and automobile traffic in ways that discourage crime. Most intruders will try to find an unrestricted way into an area. Limiting access keeps them out altogether or marks them as an intruder.

CPTED works best when combined with a comprehensive physical security program. It is important for security practitioners to be brought into the discussions early and to share their knowledge of how security can be designed from the beginning. Because many traditionalists view physical security programs as installing tools, such as locks, lighting, and alarms, they miss the important CPTED design elements. It is how the tools are used that makes the difference, and this is what the security professional will offer to the development. Essentially, the security program must be integrated into the environment, not just tools added on after the construction.

Summary
The need for physical and particularly procedural security has grown along with the development of wireless technology and an increasingly mobile workforce. Although systems may not always be the target of a malicious physical attack on an organisation, they may suffer as much as any other corporate resource as a result.

Controlling access to information system resources involves more than technical/logical controls; it also includes limiting the physical access to the resources. As organisations become more reliant on their information systems, the threats to the systems also become more sophisticated. Even with these advances in technical attacks, the basic requirements for securing the resources include front-line physical security procedures and protection.

Physical and procedural countermeasures should aim to provide identification and authentication, authorisation (access control), and accountability for all individuals who may have physical access to the system. A fourth element is the provision of physical contingency resources and alternative procedures should any aspect of the systems and the services it provides be mitigated.

Physical security should be organised in a defence - in - depth strategy: a 'layered combination of complementary countermeasures' that together present a variety of protective measures against deliberate and accidental intervention, as well as commonplace environmental threats. This can be provided in a cost-effective way by adopting measures that are already in place to address other security requirements. If so, these measures must be checked to ensure that they remain effective against the risk and that they fit with the security strategy for the system.

The effectiveness of procedural security relies on the knowledge, skills, and awareness of staff to enable them to comply with procedures consistently and completely.

Physical and procedural security are integral parts of information security and rely on integrating computer security with facilities and other forms of security.

No security solution is fool proof. We have heard of US Defence Department being compromised several times. With layered security, an organisation can delay the attack and frustrate the intruder. The fight between the security agencies and intruders/hackers is an ongoing one and will never cease. One can only hope to deter the intruders by being a step ahead and being innovative in building barriers so the core remains protected. ■