# PHYSICAL SECURITY
FACT SHEET

## Introduction

Providing a secure office space is the key to a successful business. Nearly one third of workers don't feel safe at work. This feeling of unease quickly takes a toll on productivity and office morale. Providing a safe and secure environment for your customers and visitors creates an important positive impression.

Physical security plans allow you to secure property from unauthorized access, keeping your assets and employees safe and preventing damage or loss. As the first line of defense for your building, the importance of physical security in preventing intrusion cannot be understated

## What is Physical Security?

Physical security is the protection of people, property, and physical assets from actions and events that could cause damage or loss. Though often under-appreciated, physical security is important.

The first line of defense is the building itself -- the gates, fences, windows, walls, and doors. Locking these, adding deterrents such as barbed wire, warning signage, and visible guards will put off most casual attempts on a company's sites, and that is before one enhances the level of protection with electronic systems.

# Why invest in Physical Security?

At its core, physical security is about keeping a company's facilities, people and assets safe from real-world threats. It includes physical deterrence, detection of intruders, and responding to those threats.

While it could be from environmental events, the term is usually applied to keeping people – whether external actors or potential insider threats – from accessing areas or assets they shouldn't. It could be keeping the public at large out of a company's HQ, or on-site third parties from areas where sensitive work occurs, or keeping workers from mission-critical areas such as a server room.

One of the most common errors a company makes when approaching physical security, is to only focus on the front door, using a combination of surveillance cameras, security guards and badge access, but to neglect the building or campus as a whole.

Smoking areas, on-site gym entrances, and even loading bays may be left unguarded, unmonitored and insecure. Turnstiles or similar barriers that have movement sensors on the exits can also easily be opened by putting a hand through to the other side and waving it.

# Key Considerations

When thinking about the physical security of one's building and assets, there are a number of considerations that need to be made to maximise the effectiveness of the security measures installed. These include:

1

## Identify physical weak points and determine security need

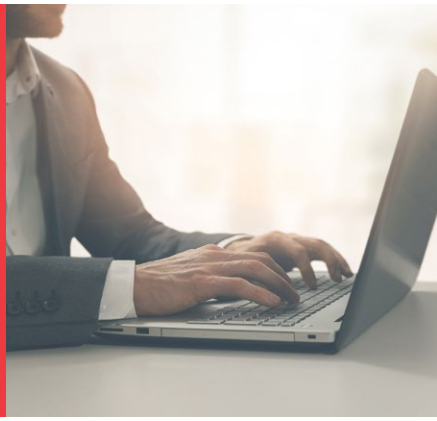
The first thing a company needs to do is work out where the vulnerabilities are. For example it is never a good idea to build high security areas against outside walls. Similarly, one needs to pay attention to what is housed above and below high security areas. By securing these weak points, companies can eliminate the most obvious threat – someone breaking in. In addition, one needs to consider installing physical barriers, cameras and access control systems to increase the physical security further.

It is also important to examine the operational processes so that visitors and contractors are not let inside sensitive areas accidentally.

2

## Keep track of all workflow processes

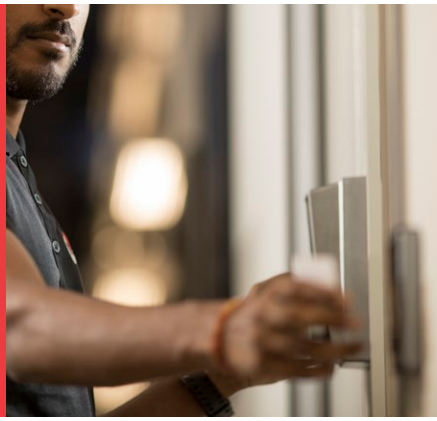
It is critical that companies keep track of their operations and compliance-related activities. It is important to limit access to only those with the right authorisation. As such, companies should regularly monitor access logs and perform audit checks.



## 3 Watch out for human error

The most common form of breach is that committed by insiders. It is now recognised that danger comes in the form of poor engineering, carelessness, or corporate espionage, but in all cases, people working in a facility pose the biggest risk. Accordingly, it is necessary that companies implement strong security policies that hold personnel accountable for their access permissions.

Employees must be deterred from lending each other's access cards, and if one is stolen, it has to be cancelled immediately. It is important that everyone understands that access should never be shared in an organisation.



## 4 Educate people on security policies

A big part of having a strong security system is staff training e.g. explaining to staff why they should not lend each other access cards and instructing them to report any suspicious activity.

Additionally, they need to understand that, for compliance purposes, workflow processes are strictly segregated and monitored. Often, regulatory agencies will want to see who accesses which piece of information and when. Eliminating duplication of access means that one is able to adhere to compliance standards with greater ease.

## 5 Layered Security

To truly secure your assets and systems companies must start from the outside in, with a layered security approach. Think of it as different lines of defence, starting from your perimeter, each with their own unique benefit.

The objective of this layered approach should be to keep out unauthorised people and if they do gain access identify them as soon as possible, keeping them contained within a secure section of the facility. Although specifics will change depending on location, these layers could include physical barriers, intruder detection, surveillance cameras, security personnel, vehicle traps, anti-drone tech, full authentication and auditable access control.

## 6 Security culture

Without doubt one of the fundamental challenges of physical security is company personnel and their attitude towards security. If they don't take it seriously, cracks will start to appear that can be exploited. To be successful, security needs to be ingrained within the culture of the business.

To achieve this, operating procedures need to be actively monitored and reviewed, regular training should be provided and working to best practise must become routine.

## 7 Backup contingencies

Finally, businesses should ensure that they have backup contingencies in place in case things like power go down. If there is an outage, do security systems still run on backup for an adequate time until the problem can be sorted? Make sure onsite backup generators have enough fuel etc.

Planning is always going to be integral here, and the more one plans, the better prepared one will be if a problem does occur.

## So What Next?

There is a lot to consider and experience counts in designing the right system. In our view, any well designed system should start with a comprehensive risk assessment. This assessment should be carried out on the basis of answering three key questions:

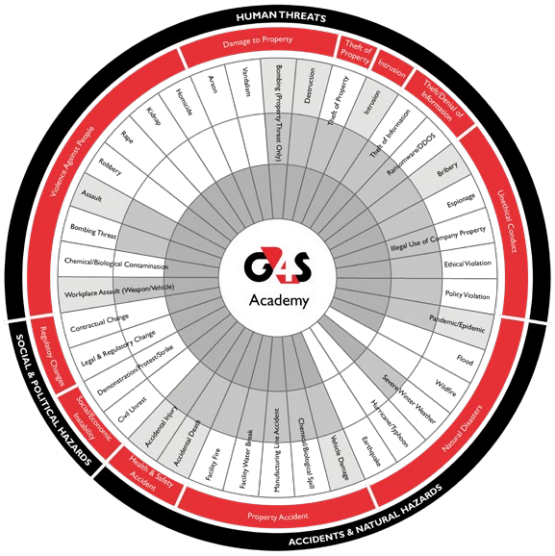
- What are we trying to protect?
- Who are we protecting it from?
- How can we most effectively protect it?

To help with this, G4S has a free online tool to provide an overview of the risks faced at

https://www.g4s.com/what-we-do/security-solutions/g4s-risk-assessment

Alternatively, we can guide you through a more comprehensive assessment.

Having agreed the assessment, we can also support you in designing the right system to mitigate the risks, using our design team that has over 120 years of experience in designing large security systems.



## If you would like to find out more please contact us:


UK: 08459 000 447 (option 1)

enquiries@uk.g4s.com

2nd Floor, Chancery House,
St. Nicholas Way,
Sutton,
Surrey,
England, SM1 1JB

Ireland: 1890 447 447

g4ssales@ie.g4s.com