CTR SecureServices

A Company Guide To Protecting Staff, Assets And Locations

CONTENTS

Introduction

This free company guide has been designed to provide valuable knowledge for an organisation to increase the safety and security of their business, with specific advice and guidance on how to protect staff, assets and locations.

OUR HISTORY

We have safeguarded various clients since 1996 and continue to pioneer how physical services and technology integrate to provide the highest levels of protection. Since inception, our company have continually tried to challenge the normal and provide relevant, cost effective and class leading security solutions. With a history of working across various continents in many security and safety related roles, we have maintained the safety and security of people and assets. We are confident in protecting our clients and finding solutions that meet their exact needs.

OUR COMPANY

CTR Secure Services is one of the leading providers of total security solutions within the UK and Europe. This is further evidenced by year on year growth since inception.

The company stands out from other competitors due to its ability to exceed customers expectations, and in addition to this being able to provide a broad and comprehensive range of security services.

OUR SERVICES

We provide an array of security solutions to secure your staff, assets and locations using our integrated approach to security, overseen with our PSOC.

- ✓ **Physical Security Operations Centre (PSOC)**
- ✓ **Protective Services**
- ✓ **Advisory Services**
- ✓ **Intelligence Services**
- ✓ **Cyber Security**

Protecting Staff

Employees are the heart of any organisation, and this is why it is vital to safeguard staff on every level, including from mental and physical harm. This guide will provide guidance on how better to protect your staff from a range of generic threats.

We will look at best practice for organisations and their staff, highlighting simple yet effective security measures.

Top Tip
Always communicate any security policy or procedure to all staff within your organisation. If they don't know about it then it's doubtful it will help them.

SECURITY WITHIN PREMISES

This section will discuss how to keep staff safe whilst they are working within your premises, this may be an office building, warehouse or any other type of facility. If you are fortunate to have some form of perimeter; then this can assist in securing the buildings and assets found inside the perimeter. Not every facility or building will have a perimeter, but if you do, then make sure it is at a standard to at least deter and delay unauthorised persons from breaching the perimeter.

Top Tip
A perimeter needs to be maintained and have adequate access control measures in place. If you have valuable assets on site, then a good perimeter will possibly deter and delay intruders.

A properly designed and implemented perimeter should:

- Increase deterrence from potential attacks
- Allow authorised access to those that require it, without hindrance
- Deny unauthorised access through intended access points
- Assist in delaying, detecting and denying unauthorised attempts to breach site security
- Provide appropriate facilities to enable security officers to carry out their duties. This should include protection in case of an attack

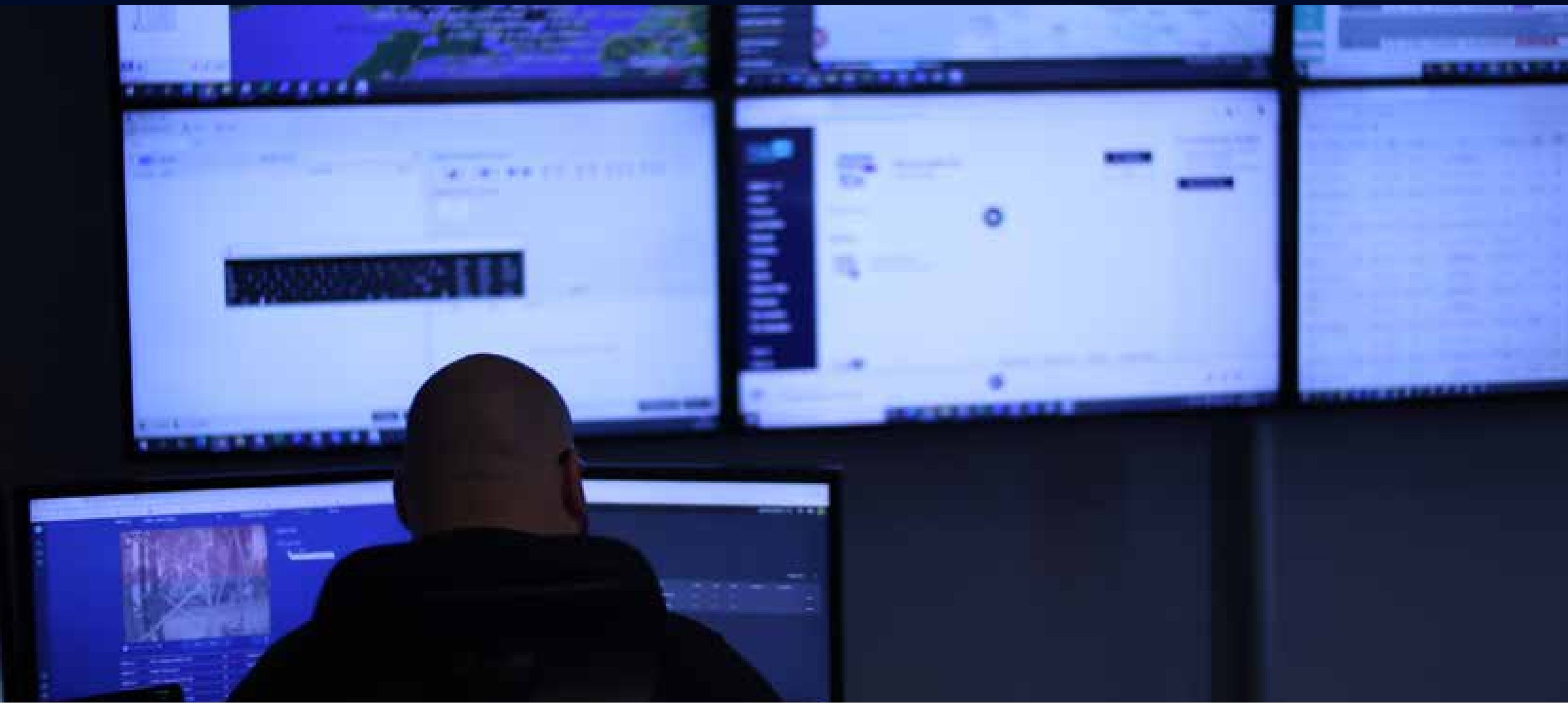
Note: We will cover more on perimeter security later.

Access control measures should be appropriate for the type of perimeter and building they are installed at and are designed to control who can go where, more importantly, who shouldn't go somewhere. Access control systems can be as simple as lock and key through to state of the art Automatic Access Control Systems (AACS).

Access control on a building is designed to keep unauthorised persons from entering; this includes those people with harmful or criminal intent. This is why it is essential to ensure that your perimeter (if you have one) and the building is secure from unauthorised access. All staff should feel safe and secure when they are at work and be protected from potential threats.

Top Tip
If you are unsure about your perimeter or building security, then CTR Secure Services can conduct an 'Intrusion Test' which will provide insight into how secure your premises are.

Security Training



Another way of increasing your employee's safety is through 'security awareness' training which can be delivered to staff through e-learning, video-based or face to face sessions. The training has the aim of increasing the awareness of staff, which in turn increases their security.

There are varying levels of security training, but all are designed to improve the knowledge of a person in terms of security and safety. The ASTA security academy has a range of courses to increase the safety of your staff; these include:

Lone Worker Protection -
https://www.astatraining.com/lone-worker-protection/

Behavioural Detection Analysis -
https://www.astatraining.com/qnuk-level-2-award-in-behavioural-detection-analysis-rqf/

Conflict Resolution -
https://www.astatraining.com/conflict-resolution/

Basic Situational Awareness -
https://www.astatraining.com/basic-situational-awareness/

ASTA can tailor any training to your organisation's specific needs, and this includes delivery methods. ASTA has helped numerous organisations in developing and increasing employee security. Training is an excellent strategy to improve security throughout your organisation.

Top Tip
Behavioural detection and active screening training can improve staff knowledge, but also assist in keeping your locations safe from those with harmful intent.

Lone Working

There are many instances of lone working, and since COVID then this way of working is becoming even more significant as more people work from home.

The definition of lone working by the Health and Safety Executive (HSE) is:

Lone workers are those who work by themselves without close or direct supervision, for example:

- as delivery drivers, health workers or engineers
- as security staff or cleaners
- in warehouses or petrol stations
- at home

If your organisation has lone workers, then you must have the processes and means to safeguard these staff during their working hours. They need to be protected physically, mentally and from online threats. This can be achieved through a range of procedures and systems, including but not limited to:

- Lone worker policy
- Check call system
- Training

Your lone worker policy should outline relevant responsibilities and highlight those who are responsible. The policy should be written to suit your specific organisation and the roles of those classed as lone workers.

CHECK CALL SYSTEMS

There are many check call systems to choose from, and ultimately you need to choose one that fits your specific organisation and budget. In this modern era, most people carry their mobile devices/phones everywhere, so many of the duty of care and lone worker systems are app-based. These are useful as if a person is going to pick something up to take with them, then it will be their mobile phone as we have all become so accustomed to carrying these devices.

This is compared to carrying a separate lone worker (panic) device. Any lone worker system aims to ensure that the staff member is safe and this is mainly achieved by the app or system sending a request to that person on a scheduled basis and for that person to then acknowledge that request. For example, an app may request that the user must acknowledge a request every two hours, if they miss one of these requests, then an alarm is raised with the organisation. There are many other benefits and technologies now in use with lone worker systems, including mapping, geo-fencing and other technological advancements.

Staff can also be provided with lone worker training which increases their knowledge of the risks associated with lone working and how to reduce such risks. Training can be delivered via e-learning or face to face with the subject content to include:

- Identifying the necessary personal security measures you may need at home as a lone worker either working from home or mobile, from the home location
- Considering travelling arrangements for getting to and from your working environment
- Assessing the safest method of transport, and how you can become safe by following some guiding principles
- Understanding an awareness system so that at certain times, or environments, your awareness will become more astute
- Dealing with aggressive people
- Dealing with violence to enable you to remain in a safe posture whilst trying to de-escalate the situation

Top Tip
Make the training relevant to your own organisation by using work-based examples, using relevant scenarios that are relatable to your staff.

Criminal Behaviour
(Criminology)

Firstly, it is worthwhile exploring why we need to protect anything at all. This can be achieved by understanding criminal behaviour and the psychology of why people commit crimes.
Why do people commit crime?

Although there is no simple answer to this, we can understand the fundamental catalysts for people to commit a crime.

CLASSICIST AND POSITIVIST CRIMINOLOGY

Two main theories on criminology are the classicist and positivist theories.

The classicist theory assumes that knowledge of the consequences of crime will be enough to be a deterrent for rational persons.

The positivist theory does not follow the classicist approach and positively rejects it. Instead, positivist criminology highlights that individuals are motivated by forces over which they have no control.

We will focus more on positivist criminology and three distinct areas, these being:

- Biology
- Psychology
- Sociology

CRIME AND BIOLOGY

Some theories and scholars argue that criminal acts can be related to a person's biological makeup, in that they have somehow not developed as much as those not committing a crime or their actions are somehow hereditary. This means that those that are criminally orientated are more savage related than the average rational person and have not developed as much psychologically compared to law-abiding people. This means they don't hold the same rational and social beliefs compared to a law-abiding person.

CRIME AND PSYCHOLOGY

Theories relating to the psychological aspect of crime argue that criminal behaviour is based on neurological disorders and/or personality issues. This could include dramatic and traumatic experiences increasing the chances of illegal activity and personality disorders. For example, someone that witnessed violence through their childhood years may result in a personality disorder that could lead to violent behaviour from themselves, which could include a criminal act such as GBH or assault.

CRIME AND SOCIOLOGY

This theory is based on social factors in determining human behaviour and criminal activity. This includes adverse social circumstances as the primary catalyst for committing criminal acts; these social factors may include:

- Financial
- Drug and alcohol addiction
- Reputation
- Social environment
- Beliefs (radical)

FINANCIAL

Poverty could be a reason why a person resorts to crime, at the other end of the financial spectrum then we would have those that are motivated by money to subsidise their lifestyles (lifestyles could relate to drug and alcohol). These examples are two ends of the scale, as someone experiencing poverty may not have many other options to feed/house themselves. In contrast, a career criminal motivated by financial gain may have options but chooses to commit a crime.

DRUG AND ALCOHOL ADDICTION

Those persons that are addicted to either drugs or alcohol would need to fulfil their needs continually, and unless they have a high level of income to support their addiction, then they may need to resort to crime. This could be in the form of theft, burglary and robbery with their addiction and social situation, forcing them to commit a crime.

REPUTATION

It is not unheard of for crime to be committed to boosting a person's reputation, especially amongst modern gangs, the social influence of others may push someone to commit low level or high-level crime from general theft through to shooting an opposing gang member.

SOCIAL ENVIRONMENT

A person's social environment can have a significant impact on whether that person commits a crime or not. This can start from persons early years where their childhood development can be critical in how they interact with the world around them. For example, a child may not initially know that stealing is wrong; a parent would have to educate them. If there is a lack of moral guidance from an early age, then it is probable that there would be an increased appetite for criminal behaviour.

BELIEFS

A person's beliefs can be a motivating factor for conducting criminal activities. At the higher end of the spectrum, we have terrorism which has been historically linked to specific ideologies, including recent extremist beliefs and the subsequent terrorist attacks that follow. Whether these beliefs are right or wrong, the effects can be devastating.

Consideration

If we were dropped in the ghetto areas of Johannesburg with a nice car and wearing nice jewellery, then it is highly accepted that we would be car jacked and robbed. Why? Because of the social environment being a highly poverty-stricken area, so the opportunity to make money through crime would be very high.

We can also explore why people **DO NOT** commit a crime, and this involves social control theory, examples are:

- Belief
- Involvement
- Commitment
- Punishment

BELIEF

A person's belief in knowing what is right and wrong may cause them to think twice before committing a crime; again, this can be linked to a person upbringing. Primary, secondary and tertiary influences can have a large effect on these personal beliefs.

INVOLVEMENT

The level of involvement that a person spends in a crime-free environment which in turn increases that person's ability to remain crime-free

COMMITMENT

A commitment from a person to live a crime-free life, understanding what is right and wrong and then making choices to continue to do what is right.

PUNISHMENT

For many rational thinking members of society, the threat of punishment is enough to keep them from committing any form of crime.

Now we have a better understanding of why crime is committed, so hopefully, this can help an organisation better understand how to protect against such crimes.

Protecting Assets

There are many different views on what an asset means to an organisation; below are just some ideas (tangible and non-tangible) of what could be classed as an asset.

- Personnel
- Products
- Data
- Vehicles and machinery
- Expertise
- Intellectual Property
- Reputation

In this short business guide, we will focus on protecting personnel, data and products.

PERSONNEL

We have already touched on protecting staff whilst they are at work, but we also need to discuss how to protect staff as an asset to your organisation and the duty of care present. There are numerous examples of how staff work within organisations, some visit the office day after day, some travel the breadth of the country day after day, and some travel around the world in their line of work. This means that your organisation must be specific in your approach to protecting your staff; this can be achieved by conducting an assessment of the modes of work that your staff may undertake.

Positive security culture must be encouraged and championed within your organisation. By promoting a positive culture then your organisation can nurture and improve personal security in all people linked to your organisation, this includes contractors and suppliers. In turn, this will increase the levels of security for your staff and your organisation as a whole.

INSIDER THREATS

Personnel are vital for an organisation, although in addition to protecting staff then you must also be aware of the potential of an 'Insider Threat'. An insider threat is a person who exploits or has the intention to exploit an organisations asset

More information on insider threats can be found here: https://www.ctrservices.co.uk/a-guide-to-insider-threats/

Top Tip
Identify enthusiastic individuals throughout the business with different levels of seniority to become champions for security within their teams.

DATA

Information must be protected from the time it is created through to the time it is destroyed (CPNI), especially sensitive information which for a business, can be most information. Organisational data must be stored securely, and this includes financial information, intellectual property, employee details and any other information relevant to your organisation. The relevant standard for information security is the ISO/IEC 27001, which provides requirements for an information security management system (ISMS). However, there are more than a dozen standards in the ISO/IEC 27001. Using them enables organisations of any kind to manage the security of assets such as financial information, intellectual property, employee details or information entrusted by third parties.

VEHICLES AND PLANT

Vehicle and plant are becoming increasingly targeted for theft and criminal damage. One of the primary considerations for any organisation is whether they have any form of vigilance over such assets. What we mean by this is whether the organisation tracks or monitors vehicles and plant machinery. Tracking devices are widely used to protect assets of this nature with trackers being professionally fitted to vehicles and plant machinery, once installed then an organisation has a level of vigilance over its assets. Not knowing if and when your assets are being stolen should not be the case in this modern age. More information on tracking can be found here: https://www.ctrservices.-co.uk/asset-person-tracking/

REPUTATION

Every organisation has a reputation to protect; this reputation is viewed by clients, customers, shareholders, competitors and the public. Although an intangible asset, it is still one of the most important assets that an organisation must protect. In particular, those organisations which are customer focused. A businesses reputation can be the most valuable asset they have, meaning that every effort should be made to protect that asset. From a security perspective, then an organisation can protect its reputation through indirect actions. This includes employing security providers that understand the need to represent the organisation professionally, safeguarding against accidents that cause damage/interference to the public and generally ensuring that the organisation is conducting itself diligently.

Protecting Locations

Wherever your organisation has one location or one hundred spread across the globe, each location should be safe and secure for your employees, contractors and visitors. This guide will not delve into every type of building or location but will highlight the areas of building and location security, which should be considered by all organisations.

Top Tip
When your organisation takes over a new building, do not rely on the security measures in place. Ensure that an assessment has been conducted to ensure security measures are relevant.

PERIMETER

If your facility has a perimeter, then this needs to be maintained to ensure effectiveness. Any security measures used in conjunction with the perimeter must be relevant and effective to ensure your facility's maximum security.

The aim of a perimeter is to:

- Deter intruders and unauthorised persons
- Assists in detection, delay, and denial of access
- Helps regulate access control
- Reduces the impact of high-risk threats

An organisation must understand how and why perimeter security measures are in place. This knowledge can be explained by our security consultants https://www.ctrservices.co.uk/security-design/

Types of perimeter include (but not limited to):

- Brick and concrete walls
- Palisade fencing
- 358 mesh fencing
- Metal railings
- Chain link mesh

An assessment should be undertaken on the perimeter and the security measures in place; this will ensure that any perimeter is effective.

PHYSICAL INTRUDER DETECTION SYSTEMS (PIDS)

There are numerous Physical Intruder Detection Systems on the market, and these can enhance the security of your perimeter. These systems can be fitted on perimeter fences to identify and alert intruders, the technology used includes:

- Vibration sensor
- Microphonic
- Wall Break
- Fibre Optic

Vibration Sensor:
This type of detection system utilises numerous sensors to identify and analyse vibration in the fence. The sensors can differentiate between cutting, scaling or even lifting of the fence.

Microphonic:
This type of detection can analyse noise patterns, similar to the vibration sensor. It can then identify the kind of intrusion from cutting through to climbing.

Wall Break:
This type of intrusion detection system is for use on a brick wall and drywall constructions. The system will detect vibrations which will allow the system to identify if the wall is being breached.

Fibre Optic:
This type of detection monitors the coherent Rayleigh backscatter noise signature in a fibre optic cable as pulsed light is sent into the fibre. It can measure small changes in the coherent Rayleigh noise structure that occurs from pulse to pulse.

CCTV (CLOSED CIRCUIT TELEVISION)

One of the most common detection systems used for business and residential premises are CCTV systems. These can provide cost-effective protection which can be monitored or recorded; monitoring provides a higher level of security, whereas recorded CCTV data can be recalled in the event of an incident.

With advancements in technology, then modern CCTV cameras can utilise SMART technology, which includes the use of various modes of detection. Most modern-day SMART cameras can use the following detection modes (but not limited to):

- Intrusion detection
- Line crossing detection
- Face recognition
- Unattended baggage detection
- Object removal detection

If installing CCTV, then an operational requirement survey should be conducted, this will ensure that the right cameras are placed in suitable locations and follow industry standards. If you plan to react to incidents detected by CCTV, then the system needs to be monitored by a professional person(s). This can be achieved internally and/or contracting an approved monitoring station which will monitor and respond accordingly. The level of response may be in the form of alerting the police or registered keyholder, whichever it is, the response should be in a timely manner. A professional monitoring company will ensure that they know your organisation, its location, buildings and procedures. This includes having a visual map of where each camera is located so that police or security response can be directed to where the threat was detected.

More information on CCTV can be found here:
https://www.ctrservices.co.uk/cctv-monitoring/

CPTED

Crime Prevention Through Environmental Design is a crime prevention theory focusing on tactical design and the effective use of built-up environments, with an emphasis on crime reduction.

A primary objective of CPTED is to reduce/remove the opportunity for crime to occur in an environment and promote positive interaction with the space by legitimate users. CPTED is a preventative, pro-active model, and not a reactive one.

CPTED comprises five principles, these being:

Physical security is the measures which are used on individual buildings to ensure that they withstand attack.

Surveillance design ensuring that residents can observe the areas surrounding their home or business. Surveillance can be facilitated by ensuring that front doors face onto the street; that areas are well illuminated, and blank walls are avoided.

Movement control which encompasses the restriction of access, egress and through movement. High levels of through movement allow offenders to access and egress an area; permits identification of targets and increases anonymity.

Management and maintenance mean that the processes are in place to ensure that development is free from signs of disorder. This signals that the area is cared for.

Defensible space means the ownership of space in a neighbourhood should be clearly defined. For example: public (e.g. pavement); semi-public (e.g. front garden); semi-private (e.g. rear garden) and private (e.g. inside the home).

As an organisation, there are many benefits to be taken from the principles of CPTED. More information can be found here: https://designforsecurity.org/crime-prevention-through-environmental-design/

Top Tip

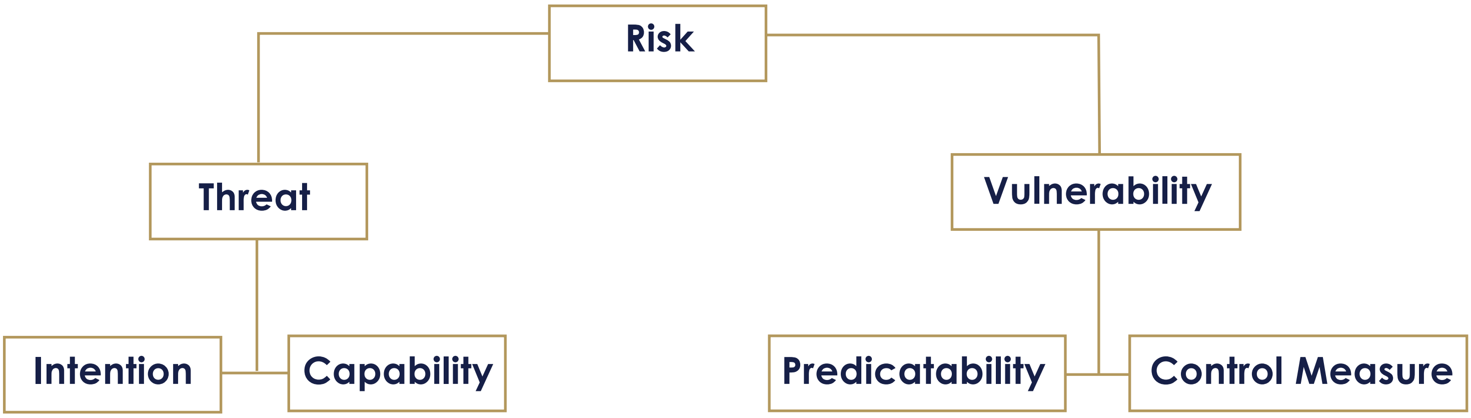
Have a walk around your buildings and facilities and think from a criminal's perspective. Where and how would you break into your own property? This will provide you with a starting point for change.

Summary

This guide has touched on some of the ways you can protect your staff, assets and locations. There is an increasing need to stay ahead of criminal intent. This means your organisation must understand the threats it may be exposed to and what your vulnerabilities are; once these are known, then you can mitigate the associated risk.

MODEL APPROACH

The approach of understanding threats and vulnerabilities that CTR Secure Services adopt is depicted below:



Risk

Threat

Vulnerability

Intention

Capability

Predicatability

Control Measure

If this guide has generated interest in how you can better safeguard your organization, then please do not hesitate to contact a member of our team.

We hope your organisation and staff stay safe throughout 2021

CTR SecureServices

A company guide to protecting staff,
assets and locations

CTR Secure Services

☎ 0203 285 8987

✉ info@ctrservices.co.uk

🏠 70 Gracechurch Street, 3rd Floor, London, EC3V 0HR