construction site security
– a guide

January 2012

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Form No. 123 Issue 1

Contents

Introduction

Construction sites are easy targets for the opportunist thief; the high value of plant and equipment can lead to quick and easy profit for the successful thief. Depending on locality, each site will have its own issues of concern. Construction sites are subject to a number of threats, against which security should be applied by the site operator. These include theft, vandalism and deliberate damage and terrorism.

Theft is common. The high value of construction plant and materials and the nature of a construction site, with its constant change and movement make this crime tempting for the opportunistic, as well as the carefully planned crime.

Vandalism is also common and may occur as a result of political or commercial concerns on the part of the perpetrators as well of mindless lust for damage and destruction.

Terrorism is potentially an issue as well; not only is there a threat of politically-motivated attacks on construction sites to delay or prevent construction; there is also a risk of terrorist pre-positioning of devices or materiel to allow or perform destructive acts after completion of construction.

Building and construction sites provide a security challenge due to their constant change; both physically in the value and accessibility of the property they contain, and the frequent access needed by a wide variety of outside contractors.

This guide is intended to provide a recommended approach to security to be taken by site operators both before and during construction and during the handover of the construction site to the eventual site operator, landlord or owner.

As every construction site will differ in terms of scale, location, duration of work and the security risks it is not possible for a single guide to cover all possibilities. The approach of this guide is to describe the techniques of threat assessment and risk analysis. The general principles of risk mitigation are then described before some practical examples are given.

1. Scope

These guidelines are designed to provide site managers and operators with an overview of the common considerations of risk assessments and security measures to be taken into account on construction sites. It is not intended to be a detailed manual, but should be used to help frame thinking about security and to outline the process to follow in preparing risk assessments and the necessary mitigation measures to be taken. In general, it is assumed that managers and operators will either have internal specialist resource to assist in the development of a security plan or will retain a security consultant to assist in this development. It is also assumed that the security operational package will be delivered by a commercially-procured third-party.

2. Terms, definitions and abbreviations

2.1 Definitions

2.1.1 Event

Occurrence or a change in a particular set of circumstances.

2.1.2 Guard Force

The term guard force in this document refers to the people with the responsibility for protecting the site. On a larger site this may be a permanent contingent of guards. On smaller sites this might be a guard patrol or an individual with responsibility for security among other responsibilities.

2.1.3 Hazard

An event with negative consequences, brought about through natural, environmental or non-malicious human intent (e.g. flooding).

2.1.4 Impact

The outcome of an event that affects objectives. In the context of this guide an impact is something that will prevent or hinder the operation of the construction site. (Also known as a consequence).

2.1.5 Raw Risk

The risk as assessed before mitigation.

2.1.6 Residual Risk

The risk as assessed after mitigation.

2.1.7 Risk

A threat or hazard assessed for likelihood and impact.

2.1.8 Risk Appetite

'The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.'
NOTE: This definition is taken from The Orange Book: Management of Risk – Principles and Concepts, HM Treasury, 2004.

2.1.9 Threat

An event with negative consequences, brought about through malicious human intent (e.g. arson).

2.2 Abbreviations

ACS Access Control System
CCTV Closed-Circuit Television
CTSA Counter Terrorism Security Advisor
IDS Intruder Detection System

3. Threat assessment and risk analysis

3.1 Introduction

Fundamental to security is the concept of **risk**. The definition of risk used throughout this guide is:
"A **threat** or **hazard** assessed for likelihood and impact"

A **threat** is defined throughout this guide as:
"An event with negative consequences, brought about through malicious human intent"

A **hazard** is defined throughout this guide as:
"An event with negative consequences, brought about through natural, environmental or non-malicious human intent"

The risks that may affect a construction site can change rapidly during the construction process and it is important to regularly re-assess the situation. For example preventing travellers from occupying an area of land may be important prior to construction but after building commences theft of materials may be more likely. To make it easier to maintain an awareness of the risks it is recommended that a register be created. The register will contain a list of all of the perceived threats and hazards and details of the actions taken with regard to each. Registers can have many forms, for example a spreadsheet or a folder with a separate page for each threat. It is important to separate the contents into two identifiable parts (although they could be on the same page):

Raw Risk Register (see 3.2)	A catalogue of the risks identified as being of concern, together with an assessment of their likelihood and impact before they have been addressed. This information forms the input to the analysis. For each risk a "Risk Appetite" is decided and then measures determined to mitigate the risk so that it is below the level of acceptable risk appetite.
Residual Risk Register (see 4.3)	Details how the measures to mitigate the risks have reduced the perceived level of risk (hopefully below the "risk appetite"). This forms the output of the analysis.

The method for completing the registers is described in more detail below.

Both registers are living documents and the process of risk assessment and mitigation is iterative, i.e. it continues constantly through the life of the project. Not only can the risks change but also the risk appetite and the available methods of mitigation. When a risk is re-assessed reference can be made to the information in the register to reduce the work required.

3.2 Raw Risk Register

3.2.1 Threat and Hazard Assessment

A useful method of threat assessment is to categorise threats and hazards by type. Hazard assessment will often include health and safety aspects, as well as contingency planning, especially where extreme weather, accident or other 'accidental' or environmental events are concerned. Nonetheless, hazard-derived risks should be included in the site risk register and their mitigation recorded just as with threat-derived risks.
Generally, threats and hazards fall into these categories:

- Threats to life
- Threats to property and assets
- Threats to operations

This categorisation may be helpful when first considering the range of threat and hazard to which a site or development may be subject.

Typical threats for a construction site
Threats that may be considered typical will vary according to the type and location of the site. The following are suggestions but each site will be individual. • Theft of plant • Theft of fuel • Theft of materials from the site • Vandalism • Arson • Breaches of security into existing buildings • Robbery or attacks on the construction workers • Reconnaissance of development to discover details of completed building • Bombs (perhaps planted for detonation after completion) • Intruders intent on committing suicide • Protesters (either related to the site activity or simply for publicity)
Whilst considering threats the risk assessment should take into account hazards. In part this is because the methods of mitigation (see below) may help for both threats and hazards. The following hazards are typical: • Flooding, storm damage, etc • Landslide, earthquake, etc • Project issues (Staff injury, Failure of supplier's business, Finance, etc)

3.2.2 Risk Analysis

As noted above, risks are threats or hazards, analysed by likelihood and impact. For assessment purposes, a number of methods may be employed to 'score' these; generally, it is suggested that a simple traffic light system (Red-Amber-Green) may be best used, as numeric scores give a false impression of precision. Whichever means is used, the risk score is the product of **likelihood** x **impact**.

It is important to bear in mind that impact may take various forms – some impacts are straightforward and are defined by danger to life or property, others are less tangible and may involve reputational impact which might, for example, reduce shareholder value in a company or damage reputation sufficiently to impact the winning of new business.

For example, a given threat – perhaps opportunistic pilferage from site – will be assessed. The likelihood is quite high (bearing in mind that this initial assessment will be conducted on the basis of things as they are at the time, not as they will be after mitigation), but the impact is relatively low. Using rough numeric values, a high likelihood is 5, a low impact is 1 – the risk score is thus 5 x 1 = 5. Referencing the table below, it can be seen that the resultant raw risk is Amber. Note here that the precise numbers used will vary according to the risk appetite (see below) of the assessor. Also note that likelihood is often conditioned by local circumstances and demography, as well as relative attractiveness of target assets to criminals or other malicious elements.

Risk Score	Categorisation	Notes
0-1	White	No significant risk
2-4	Green	Low risk – **may** be mitigated
5-10	Amber	Medium risk – **should** be mitigated
10+	Red	High risk – **must** be mitigated

3.3 Example Raw Risk

If we consider the threat of theft of fuel then the details in the raw risk register could appear as follows (the actual details will be specific and different for each site).

Raw Risk Register (Sample extract)		
Risk	Theft of fuel	
Owner	Site manager	
Description	Fuel used for vehicles and generators is a desirable commodity for thieves as it is not easily traced and is of relatively high value. During and following theft of the fuel it is likely that fuel will be spilled causing environmental damage with associated clean up costs. Loss of fuel may prevent operation of machinery causing delays. Damage to fuel tanks will be costly to fix.	
Likelihood	Very high (5/5)	
Impact	High (4/5)	
Raw risk		= Likelihood x Impact, 5 x 4 = 20. High Raw Risk (must be mitigated)

3.4 Risk Appetite

A key concept to understand is that of risk appetite. A site operator or manager must understand the extent to which he is comfortable with carrying risk – i.e. to what extent he is prepared to commit resource to mitigate risk and what level of risk he considers acceptable. Without this understanding and without tying the risk register and risk rating to risk appetite, risk assessment, analysis and management will become an empty exercise.

Continuing our example of fuel theft we may consider that the risk appetite is rated at perhaps 5 (out of 25). It would be wrong to assume that the risk appetite is going to be zero. Achieving a zero residual risk normally involves a high cost in terms of security measures that might be more costly than suffering the loss.

4. Mitigation

4.1 Introduction

Once raw risks are assessed and categorised in order of severity in the raw risk register, mitigation should be applied. Broadly, mitigation may take three forms:

- Ignore / Accept
- Export / Transfer
- Address

Ignoring a risk is sometimes appropriate, where the cost (in terms of financial or resource exposure) of any mitigation exceeds the impact of the event which defines the risk. Risks should only be ignored, however, after careful analysis of mitigation cost and impact. Ignoring a risk means that no action is taken to counter it but does not mean it is forgotten. Such risks should still be reviewed in case the situation has changed.

Exporting a risk can be performed through insurance or contracting of a third party to deliver mitigation. While this is entirely sensible, for example, where this can be done for the expenditure of less resource than if directly mitigated by the operator or manager, it is important to remember that this does not export responsibility for, or ownership of, the risk, but merely for its management. This presents a risk in itself, in that management of the risk falls mainly outside of the control of the operator or manager.

Addressing a risk is the application of mitigation measures directly by the operator or manager. Generally, this will involve the application of people, processes or technology to an issue to reduce the impact or the likelihood (or, ideally, both) of a risk, in order to bring its rating down to below the operator or manager's risk appetite. This document necessarily concentrates on direct addressing of the risk.

Using the numeric risk analysis method briefly described above, if we consider a raw risk with a likelihood of 4 and an impact of 3 then we have a risk score of 12. Let us assume that a risk appetite of 4 is accepted. This means that to address the risk mitigation measures should be put in place so that either the likelihood is reduced from 4 to 1, the impact is reduced from 3 to 1, or a combination of mitigation reduces both to at most 2. The risk after mitigation is the residual risk.

Whilst it may be possible to reduce the risk to a very low level ("zero risk"). The cost of doing so may be higher than the impact or the method of mitigation could itself have an unacceptably negative impact on the operation. This is a possibility that should always be considered and included in any assessment.

It is impractical to protect a construction site against every conceivable threat. The strategy used should be based on an assessment of the risk of each form of threat considered against the relative costs of protection (i.e. the mitigation).

On some sites of critical national importance it may be necessary to identify everybody entering the site and to carry out searches. This may also apply for health and safety reasons or for working in dangerous environments such as tunnels.

4.2 Mitigation Strategies

Mitigation strategies selected may include the following:

- Restriction of access to site
- Surveillance of persons on site
- Protection of site assets
- Site safety provisions
- Provision for controlled and monitored site evacuation
- Liaison with police, local authorities and other stakeholders

Generally, a construction site will have some, or all of these measures applied. Particular characteristics of greenfield and brownfield sites will have an influence on which, and how, measures are applied.

Greenfield (new build) sites will give the operator or manager maximum flexibility in deployment of both physical and operational measures to mitigate risk. The site can be laid out and designed in such a way as to maximise advantage from, say, perimeter fencing, or surveillance and thus provide good security at minimum cost.

Brownfield (redevelopment) sites will often constrain the operator or manager either to compromise site security through unchangeable elements of the site layout or devote relatively more resource, in terms of physical barriers or operational measures, to provide appropriate security than would be the case in a greenfield site.

In either event, it is important that the risk mitigation plan be designed in close cooperation with the site manager or other entity responsible for site planning and operation and that both sides remain in dialogue in order to ensure maximum value is obtained from the sometimes significant resource investment required. It should always be borne in mind by the security planner that the aim of the exercise is to allow the operation of a construction site and that security measures should, as far as possible, support this.

4.3 Residual Risk Register

As previously described, the information about the assessed risk following mitigation, the "residual risk", should be recorded in a Residual Risk Register. This facilitates the updating of the risk analysis following changes in circumstance.

4.4 Example Residual Risk

If we continue the consideration of the threat of theft of fuel then the details in the residual risk register could appear as follows (the actual details will be specific and different for each site).

Residual Risk Register (Sample extract)		
Risk	Theft of fuel	
Mitigation measures	1. Restriction of access to site (as part of general measures). 2. Addition of surveillance and on site guards (as part of general measures). 3. Reducing the amount of fuel stored on site. 4. Parking and fuelling of vehicles in a more secure location off site where possible. 5. Remaining fuel storage in a secure compound.	
Residual likelihood	Low (1/5) The overall effect of the measures should significantly reduce the likelihood,	
Residual impact	Medium (3/5) Impact is less because quantity of fuel on site is reduced.	
Residual risk		= Likelihood x Impact, 1 x 3 = 3. Low Residual Risk

The residual risk is now within the agreed risk appetite (4/25) but as noted the risks can change. For example at some point in time the secure compound around the fuel store may have to be removed and use temporarily made of a fuel bowser thereby significantly increasing the likelihood of theft.

5. General principles of mitigation

5.1 Deterrence, Detection, Delay and Response

Successful crime prevention strategies should aim to reduce the risk to the construction site by increasing the risk to the thief or other criminal. The types and level of security and protection used should be determined by the results of the risk assessment. Consideration should be given to the use of the site and the level of security should reflect the time when the site is most at risk.

A simple piece of advice is to not to place all hope in a single solution. Security provisions should be used in combination to achieve four things: Deterrence, Detection, Delay and Response. In many cases a solution will contribute to more than one of these. For example, a strong fence will deter a burglar and also cause a delay gaining entry.

Deterrence

Deterrence takes many forms. A ramshackle site will appear easier to break into and may imply less protection. Alternatively the fitting of solid fencing, high quality locks, intruder alarms, CCTV and signs advertising guard patrols shows a potential thief that the owner takes the issue of security seriously and may make them go elsewhere.

Detection

Detection is the identification of the presence of a threat such as a burglar. Identification is used in two senses. There is the immediate identification to alert those affected by the threat or request response by protectors (e.g.

the police) and there is also the use after an event to identify criminals. The latter does not just mean CCTV. Detection can include monitoring of visitors to ensure only authorised people are on site.

Delay

One view is that no barrier is impenetrable if an attacker is determined enough to break it. The measure should therefore be in terms of the delay provided. The fitting of an intruder alarm will detect a crime but will not prevent theft unless sufficient delay can be caused to slow the action of a burglar. Any delay during the committing of crime increases the danger to a criminal that they will be caught and therefore acts as a deterrent to completion of the crime. It is not just whether a solution can be defeated that should be taken into account but how long it takes to defeat and what effort is required.

Response

If a criminal is not completely deterred then at some point a form of response is required. Response could be actions of a security guard or the arrival of police. To determine the security provisions the form of response must be known. If it is going to take fifteen minutes for guards or police to arrive then the delay provided should match this.

5.2 Layered Security

The principle of layered security is basically not "putting all your eggs in one basket". The idea is to spread the security features in an appropriate way. This means starting with the property boundary and considering each possible feature on the route to the most secure location. For example returning mechanical plant to a central compound means that a shorter length of more expensive fencing can protect it.

Security can be compared to the layers of an onion made up of a series of physical security measures, starting with a perimeter fence or barrier with controlled entry points. Each layer may be used in combination with electronic detection systems. This means that, after overcoming one layer, detection methods can prompt for a response to arrive while the next layer delays the criminal.

6. Securing the site

This section covers specific measures which may be applied to secure a construction site. The bulk of the approach used covers crime, whether opportunistic or planned, as these measures will also mitigate against 'routine' terrorist risks, invasion of the site by protestors or the need to exclude those intent on suicide.

Where the risk of terrorist attack is considered significant (for example, where the facility under construction is likely to be a terrorist target, or one of the commercial entities participating in the project is itself a terrorist target), operators and managers will have been made aware of this and police and other external stakeholders will take a proactive approach to supporting the site security operation, probably through the local police Counter Terrorism Security Advisor (CTSA). It is good practice to consult the local CTSA in any case and it is recommended that security planners at least make courtesy contact with these (through the responsible local Police area) when planning is complete.

6.1 General Guidance

Security is applied through the application of physical and operational measures. Physical measures are infrastructure designed and deployed to support security; operational measures are those human activities and processes designed and performed to support security.

6.2 Physical Measures

These fall generally into the following fields:

- Containment and Obstacles (fences, barriers, bollards, gates, secure storage etc)
- Technical Systems (lighting, CCTV, access control systems, intruder detection, asset management and control systems etc)

6.2.1 Containment

Containment is applied to the perimeter of construction sites, to delineate the area under control, prevent accidents to non-site personnel and to deny access to unauthorised personnel. Dependent upon circumstances and requirement, actual perimeter design may take any number of forms, although it is recommended that part of the mitigation strategy development include definition of required containment. Appropriate standards with which suppliers should be invited to comply will be found below.

Gates and other perimeter openings should also be designed in such a way as to permit control – and blocking – of inbound and outbound foot and vehicular traffic. By virtue of their nature, construction sites see many vehicle movements in and out and each movement represents a discrete threat. It is recommended that busy/high value sites consider protection of vehicular interfaces through the perimeter with deployable traffic control measures such as gates or mobile bollards (a list of appropriate standards can be found later in this guide).

High-value assets are necessarily often left on site when the site is unmanned or partially manned. Consideration should be given to secure storage for high-value tools and equipment and for control and secure parking of high-value plant. It may be appropriate to establish contained and secured parking areas (where space and resource permits) for such items of high-value plant.

Procedural issues for construction sites

Providing the containment for a site is a first step to improving security but it is important to ensure that the workers on site realise the importance of returning plant and materials to the secure areas. Always ensure that keys for vehicles are not left in them and are secured properly when not in use.

6.2.2 Technical Systems

Technical Systems, where deployed, should be properly integrated in the overall security plan. Surveillance systems (i.e. CCTV) can have a deterrent effect and can be used to good effect for forensic purposes and for monitoring of the site for health and safety purposes. When used with a suitable, planned response capability surveillance systems can provide good mitigation of many security risks. It is important to note that, when procuring systems for deployment on a construction site, the requirement for physical robustness and resistance to dust and water ingress is extremely important.

Surveillance systems also require lighting to be effective – and lighting also has a key role to play in supporting security operations (see below) and site health and safety. Lighting should eliminate impenetrable shadow at key locations and consideration should also be given to the need to minimise light pollution, possibly through focusing of lighting downwards and inwards into the site or development – and to the need to limit excess energy expenditure. Use of photo-electric activation, which allows lighting to remain inactive when ambient light levels are at an acceptable level, should be considered.

Access control systems (ACS), where deployed, using database-driven identity management and token-based access, allow not just control of access, but also up-to-date and accurate accounting for personnel on site. This greatly aids health and safety. There is an administrative overhead on management of these systems and the requirements for robustness above apply equally to them, but the cost-benefit ratio is usually sufficiently compelling for a larger site to elect deployment.

Intrusion Detection Systems (IDS) have a role to play in the control of perimeter segments or areas of sensitivity not covered routinely by other surveillance, whether electronic or other.

Alarm Systems take the form of covert alarms, which are designed to alert the security staff of breaches and allow them to take reactive measures and overt alarms, which may be used to signal to site occupants, notably for evacuation purposes.

Communications Systems take in both fixed (telephony) and mobile (radio, cellular) communications systems. On larger sites, it is assumed that the guard force will have use of its own dedicated security communications systems.

All infrastructure (network cabling, switching, power supply, antennae etc) deployed to support technical systems should be protected in its own right from damage, whether applied through environment, vandalism or deliberate attack. Vital infrastructure should be securely contained and access limited to authorised personnel only and consideration should be given to protecting cable runs and cable containment systems similarly. All equipment deployed on a construction site should be robust, weather- and temperature-resistant and be capable of continued operation under challenging environmental conditions. It should be noted that this protection should also extend to protection of security-related IT systems and their connecting networks and that best practice IT security measures and associated policies must be applied to these. In addition, it is necessary that the systems operator also ensure that Data Protection Act and Computer Misuse Act protection is in place through technology and policy. This must be explicitly demonstrated to the site operator or manager before final introduction into service of these systems.

Technical Systems on Construction Sites

The temporary nature of construction sites including issues such as lack of continuous mains electricity and constant movement of cables and supports should be considered. Battery powered devices are available and the use of wire-less equipment can alleviate some cabling issues. Wire-less systems can also be quicker to deploy and easier to move as the site develops. Care is needed to ensure detectors and CCTV views are not blocked by stored materials (either accidentally or as part of a deliberate action).

Equipment on construction sites is also subject to all environmental elements and the likelihood of damage from the normal activities on site.

6.3 Operational Measures

These fall generally into the following categories:

- Guarding Activities
- Policy and Process

6.3.1 Guarding Activities

These are the actions performed by the guard force (typically provided by a third party under contract to the site operator or manager). They typically include patrolling, static guarding, in- and out-processing of personnel and vehicles, management and operation of technical systems, generation of response to incidents and issues and liaison with the site operator or manager.

It is clearly important that the guard force is thoroughly trained and qualified to operate all equipment and perform its duties. It is equally important that the site operator or manager makes appropriate arrangements for the management of the provision of the guard force and that regular liaison is undertaken to ensure consistency of standards and quality of performance, measured against the service level agreement which will underpin the guard force service contract.

Where the guard force is not directly employed by the site operator, it is the obligation of the security guard force provider to ensure that all guarding staff deployed on site hold a current Security Industry Authority (SIA) licence to meet the legal requirements set down under the Private Security Industry Act for employment in the private security industry. The site operator should also be aware that it is illegal to employ a contract guarding service whose security guards do not hold SIA licences. The contracted guard force will carry out their duties in line with the current British Standards for security guarding and any other criteria required under the contract with the site operator or manager.

6.3.2 Policy and Process

All security operations on site should be performed in accordance with the Site Security Policy, which should be owned by the site manager or operator and which will support a number of processes. These processes should be developed by the guard force operator in agreement with the manager and operator and should underpin the Site Security Policy. These processes should be managed, monitored and their performance measured and form part of the service level agreement above.

The Site Security Policy should explicitly state the requirements of site security and the means and extent of its enforcement. It should define, for example, the classes of person to be granted access, the requirements for gaining site access (such as agreement to exit searches, for example), the powers of the guard force and all other requirements for security. A clear condition for site access must be explicit acceptance of the Site Security Policy and persons not accepting it should be denied access.

The Site Security Policy should also cover the obligations and responsibilities of personnel employed on or visiting the site. This should include traffic circulation, responsibility for reporting safety or security breaches and the requirement to cooperate with the guard force.

7. Case Study

A large construction company had taken what it thought to be adequate security measures for a school construction site in that it was totally enclosed by a close-board fence, access was through turnstiles for workers and an air-lock for vehicles, they had installed remotely monitored (but not recorded) CCTV and there was a manned guarding presence 24/7.

The site had a history of sporadic unauthorised access by young people. However, during a weekend of the spring half-term several young people gained access to the site and caused tens of thousands of pounds worth of damage to the fabric of the building. When challenged by the security guards, they subjected the guards to verbal abuse and threw bricks and scaffolding poles at them.

The same thing happened on the following weekend. The police were called, and whilst good descriptions of the offenders were provided, no arrests were made.

A BSIA Security Consultancies Section member company was asked to provide advice and guidance. They recommended that a “Security Partnership” be formed with the school, local police and the construction company, to help educate young people on the dangers of construction sites. The CCTV cover was adjusted and included image capture to “identification” standards, which was then used by the school and police to identify the culprits. Better lighting was installed and the manned guarding contract was changed to include dog-handling duties.

The incidence of unauthorised access to the construction site by young people was significantly reduced.

8. Practical suggestions for addressing risks

8.1 Introduction

This section outlines a number of practical suggestions that could be employed as methods of risk mitigation. This list is not exhaustive and not every suggestion will be practicable in all cases. It is recommended that site managers make use of consultants to give expert advice about security measures and solutions. Independent consultants, i.e. those not promoting their own products or services, will give the best advice. Whilst security measures can sometimes be seen as an expensive grudge purchase the use of a consultant with knowledge of construction site operation can prevent wasteful and unnecessary purchases and can lead to overall cost savings.

8.2 Site Access

Apart from the desire to ensure that criminals do not enter a site, there exists under The Construction (Design and Management) Regulations, 2007, a duty for the principal contractor to "take reasonable steps to prevent access by unauthorised persons to the construction site".

One action is to minimise number of vehicles on site. By ensuring that only authorised vehicles are on site it makes it more obvious when other vehicles are present. Even users of authorised vehicles may be criminals, as may be those working on site. If possible construction workers should park off-site and enter on foot. Ensuring that all deliveries are scheduled in advance and access by delivery vehicles logged the amount of vehicular access can be minimised.

Minimising the number of entrances and the use of full-height turnstiles can restrict workers and others entering a site on foot. Entrance can be controlled by guards or electronic access control measures which can use PIN codes, magnetic cards, proximity tokens, biometric devices or a combination of these.

8.2.1 Boundary hoardings

Where appropriate, perimeter hoardings should be installed to protect the peripheral space around the construction site or building. Flat sided hoardings are considered better than fences because they are more difficult to climb and prevent viewing of the site interior. It is recommended that hoardings or fences should be a minimum height of 2.4m and high security fences at least 3m.

Where fences are used the type selected should not help climbers by offereing hand and foot holds.
Avoid temporary fencing where possible.

Angled extensions ('Fans') on top of hoardings make climbing difficult and can reduce problems with material (including litter) being thrown over the hoarding and potentially damaging materials or injuring site workers Intruders may also attempt to burrow under a boundary. Placing hoardings along existing concrete surfaces can deter against this.

Viewing windows in hoardings have advantages and disadvantages. On the positive side they allow curious people to see the site without trying to climb hoardings. It also means that criminals can be spotted by passers-by or patrols. If the visible area has nothing to attract criminals then it acts as a deterrent to crime. As a negative they allow criminals to view the interior and observe site contents and plan attacks.

Bear in mind that intruders could stand on top of vehicles or other objects (e.g. waste bins) to gain access. If anti-climb features (e.g spikes, barb wire, etc) are fitted then the lower the fence the more likely that the owner will be required to take further action (such as provision of signs) or they will be breaking the law. Your attention is drawn to the Occupiers Liability Act 1984.

For long-term construction projects with a relatively fixed boundary and high risk of intrusion it may be appropriate to consider the installation of a perimeter intrusion detection system (PIDS).

8.2.2 Gates and Entrances

Minimising the number of entrances and the use of full-height turnstiles can restrict workers and others entering a site on foot. Entrance can be controlled by guards or electronic access control measures which can use PIN codes, magnetic cards, proximity tokens, biometric devices or a combination of these.

It is recommended that there not be gaps underneath gates.

Hinges on gates should be designed to prevent the gate from being lifted free; they should also be shielded from use as steps to scale the fencing. Gates should be secured by a lock conforming to BS 3621 protected by lock protection plates welded to the gate and the frame or by a padlock and padlock fittings conforming to grade 5 or 6 of BS EN 12320.

8.2.3 Barriers

Where a perimeter fence is considered vulnerable to penetration by ramming with a vehicle, provision of a purpose designed vehicle barrier such as a trench, a high kerb outside the fence, or a series of substantial steel posts just inside the perimeter should be considered.

8.3 Lighting

Lighting can be a deterrent to site intruders and a positive aid for patrolling security staff. Lighting should be sturdy and resistant to adverse weather conditions, tampering and vandalism. Directing the lighting inwards should be considered, as it will reveal intruders either directly or by silhouette. Additional lighting may be required to ensure that all possible entrance and exit points are illuminated.

To ensure that security lighting is effective, it should be used at all relevant times. The use of a photoelectric cell, which switches on when daylight fades and off when it returns, is suitable.

Wiring for security lighting should only be accessible to authorised persons. Cables for perimeter installations should be buried with the supply for individual luminaries, teed-off through a fused spur. Exposed cables should be enclosed in a steel conduit. An interference detection circuit connected to an alarm may also protect cables. Security lighting systems should be routinely inspected and maintained.

8.4 CCTV Surveillance Systems

CCTV can be used to aid the security of a site and can act as a deterrent to criminal activity. It is important that the intended use of the CCTV system is known at the planning stage as this will affect the type, quality and quantity of equipment required. The availability of power to the CCTV system and lighting should be considered. Many different types of equipment are available with low light or infrared operation or combined with white or infrared lighting units.

CCTV images can be recorded or monitored on site or monitored remotely.

Portable CCTV systems are available that can be rapidly deployed or moved around a site for temporary or short term use. These can be wireless systems that include the capability to transmit live or recorded images to a hand held PDA, laptop or to a remote video response centre (RVRC). By combining detectors with CCTV it is possible to enhance the performance of the system by alerting those monitoring the system that there is an event to pay attention to. The applicable standard for this is BS 8418.

Remote operations can include the ability to control the direction and view of a camera using pan, tilt and zoom (PTZ) mechanics. It is also possible for the system to include integrated audio amplifiers and speakers to allow the remote operator to issue commands, for example to warn intruders to leave a site.

It is recommended that cameras are mounted on masts but it is possible on a construction site to make use of existing structures or tower crane towers, etc.

8.5 Security Guards

The use of guards has already been mentioned in 6.3 Operational Measures. On larger sites the use of 24 hour manned guards may be appropriate whereas on smaller sites the use of a guard patrols, particular night patrols can be beneficial.

8.6 Scaffolding, Ladders and Stair towers

Use scaffold protection beams to detect people attempting to climb scaffolding.

Ladders should be protected to protect climbing (e.g. by chaining planks to stop use of the rungs) and also against theft as they are often stolen to enable crimes to be committed elsewhere.

As with ladders and scaffolding, stair towers should be protected to avoid their use by intruders. It is important for health and safety reasons that semi-permanent stair towers are properly assembled and the possibility of unauthorised persons attempting to dismantle or relocate the towers should be reduced. Suitable clamps and locks should be used for this purpose.

8.7 Tower cranes

Additional security surrounding the base of tower cranes should be considered to prevent access to the tower. This may include construction of a welded cage up to 3m high with secure locks (e.g. combination locks) on access gates.

8.8 Vehicles and plant

The amount of plant on-site should be minimised. Construction sites should not be used as storage areas for other plant used at other locations. Outside of working hours move plant to a more secure compound or cage (either inside the site or at a nearby location). Road construction sites are particularly vulnerable because of their size and the inability to provide perimeter hoarding. In this case the use of extra measures is more important.
If possible store vehicles and plant out of sight of criminals.

Cover windows with locked grilles, shields or plates to prevent smashing of the glass (for attempted theft or vandalism). Immobilise vehicles or plant using physical security (chains, clamps, towing hitch locks), mechanical or electronic devices. Careful arrangement of certain vehicles (such as positioning of the buckets of backhoes and excavators) can assist with immobilisation. Purchasers should ensure (by referring to a consultant) that electronic immobilisers are suitable for the working conditions of the equipment. Electronic immobilisers can be operated remotely. Hydraulically powered equipment can also be fitted with hydraulic immobilisers. Vehicles and other equipment may also be fitted with audible alarms although the usefulness of these depends on the location of the construction site.

Tracking devices can be fitted. Although these do not prevent theft, by advertising their use thieves can be deterred. A variety of different types exist. Tracking devices and plant registration schemes can both be of great benefit for retrieving stolen plant and deterring criminals.

Use a secure property marking and registration system from a properly accredited organisation to mark tools and parts of vehicles and plant. The combination of robust marking technologies and registration on a secure database with a 24/7 verification service enables the legitimate owner of the property to be identified. It reduces the value of items to thieves and acts as a deterrent to theft in the first instance. The Loss Prevention Certification Board (LPCB) and Thatcham Quality Assurance provide appropriate accreditations.

The **CESAR** Scheme (the **C**onstruction & Agricultural **E**quipment **S**ecurity and **R**egistration **S**cheme) is the official security marking and registration scheme for all plant and agricultural equipment (**www.cesarscheme.org**). The Scheme is supported by the Home Office and ACPO and promoted by the Construction Equipment Association (CEA) and the Agricultural Engineers Association (AEA). Asset marking using this important scheme is now fitted as standard at no cost by most major construction and agricultural equipment manufacturers and receives support from most of the leading insurance companies. The scheme has proved to be a powerful deterrent to theft and a vital aid in the identification and recovery of stolen plant and equipment.

In addition, cars and commercial vehicles can be protected by window etching and registration, provided as a standard feature with various vehicle brands sold in the UK and available in the automotive aftermarket. Accredited suppliers can be found at **www.thatcham.org**

A particular threat on a construction site may be the theft of a catalytic converter from a van or other high ground clearance vehicle. Consideration should be given to the marking and registration of this item and to fitting it with a physical protection device.

In general marks added to assets may be overt (easily seen) or covert (hidden, so that attempts by the criminal to overcome the mark are hampered). To act as a deterrent covert marks require additional signage.
A method sometimes used to mark vehicles is to add extra VIN plates thereby increasing the efforts required by criminals to remove them.

Use of a company paint livery or addition of company logos can deter theft in comparison to retaining the plant manufacturer's paintwork.

8.9 Site offices

Huts should include protection against fire both because of operational hazards and the possibility of arson. Consideration should be given to the use of steel huts with steel doors, multiple locks and fold over window shutters locked from inside the hut.

8.10 Protection of existing / completed property

For construction work involving alterations to existing buildings it is important to consider the security implications affecting those buildings.

When handover of a construction site is delayed or other buildings on site are vacated during construction it may be appropriate to consider the securing of buildings by security doors and screens. Temporary alarm systems can also be used. Vacant or void property security companies specialise in provision of this type of security.

8.11 Small tools

Steel tool vaults with shielded padlocks can be used for storage of tools. Ensure that these vaults cannot be removed in their entirety.

8.12 Materials and fuel

Thieves can sell all building materials fairly easily but metals and fuel are particularly high value targets. Ensuring that metals such as cable and copper tubing are hidden from view and stored in locked containers is recommended. Likewise fuel stores should be protected as well as fuel in vehicles.

8.13 Police Liaison

A number of different activities could cause disruption to a construction site and increase the likelihood of a security risk. Good liaison with the local police can alert site managers to potential problems. Examples could be crowd trouble at local sporting events, political demonstrations, etc. These are just part of the environment and not related directly to the construction. Where the construction site itself may the target of activists (e.g. animal rights or environmentalists) then greater liaison is recommended along with the engagement of expert consultants.

9. Bibliography

9.1 Referenced Documents

Computer Misuse Act, 1990
Construction (Design and Management) Regulations, 2007
Data Protection Act, 1998
Occupiers Liability Act, 1984
Private Security Industry Act, 2001

9.2 Further Reading

9.2.1 Recommendations from BSIA

The BSIA publish a large number of guides related to Access Control, Property Marking, CCTV, Physical Security Equipment, Intrusion Alarms, Security Guarding and many other areas of security.

For further information refer to www.bsia.co.uk/publications

9.2.2 Other Guides

Plant and Equipment Theft: A Practical Guide, 2007, The Off-highway Plant and Equipment Research Centre (OPERC)

9.2.3 Risk Management – Risk Assessment Techniques

- **BS EN 31010:2010:**
  Risk management. Risk assessment techniques.

9.2.4 Fencing

- **BS 1722 series, including:**
  Fences - Specification for chain link fences.
  Steel wire and wire products for fences.
  Zinc - and zinc-alloy - coated steel barbed wire.
  Specification for strained wire and wire mesh netting fences.
  Specification for electric security fences.
  Design, installation and maintenance.
  Steel wire and wire products for fences.
  Steel wire welded panels. For fencing.

9.2.5 Locks and Key Systems

- **BS 7984:2008:**
  Key-holding and response services. Code of practice.

- **BS 3621:2007+A1:2009:**
  Thief resistant lock assembly. Key egress.

- **BS EN 12320:**
  Building Hardware. Padlock and padlock fittings. Requirements and test methods.

9.2.6 CCTV Systems

- **BS EN50132 series:**
  Locally controlled CCTV systems for use in security applications.

- **BS 8418:2010**
  Remotely monitored and detector-activated CCTV systems.

- **BS 8495:2007**
  Code of Practice for Digital CCTV recording systems for the purpose of image export to be used as evidence.

9.2.7 Access Control Systems

- BS EN 50133 series:
  Access Control

9.2.8 Alarm Systems

- PD 6662 (including BS EN 50131 series, BS 8243, DD 263)
  Alarm systems. Intrusion and hold-up systems.

9.2.9 Security Guarding

- BS7499:2007
  Static site guarding and mobile patrol services. Code of practice.

- BS7958:2009
  CCTV Management and operation. Code of practice.

Acknowledgements

The Security Consultancies section of the BSIA acknowledge the input to this guide made by Henrik Kiertzner of KRS Consulting

Construction site security checklist

This checklist is designed as a tool to help conduct a crime risk assessment for construction businesses. It is intended to help identify internal and external crime risks at construction sites and the buildings associated with a construction business, and to make suggestions for improvement if needed. The checklist may be adapted for individual needs.

No.	Item	Yes	No	Further action needed
CRIME PREVENTION COORDINATION				
01	Has a crime prevention coordinator been designated? • This should be someone that can serve as the direct liaison with the Police • This person should be someone with management level communication such as the Project Director or construction manager • All construction site losses should be reported immediately			
02	Do you have the names and contact numbers for responsible persons during non-working hours?			
ASSET AND PROPERTY IDENTIFICATION				
03	Are all assets on the construction site marked? Suggestions: • Identification number • Corporate logo or spray paint of a distinct colour displayed • Large equipment or plant should be marked in two prominent places and one additional covert place.			
04	Have all tools, equipment, and machinery been identified and asset registered? This should include: Make, Model, Serial number, Owner applied Identification number, and Value of each item.			
05	Do all employees have their personal property (e.g. tools) marked with their own unique identification number?			
06	Is there signage to indicate that all assets on the construction site have been marked and registered?			
INVENTORY CONTROL				
07	Have procedures been established for checking material on and off the construction site?			
08	Are there processes for maintaining inventory control of all materials and tools delivered to site? Each invoice/delivery note should be carefully checked for accuracy. Shortages or overages must be reported.			
09	Are materials and equipment checked frequently?			
10	Has a member of staff been made responsible for supervising waste disposal? Remove empty crates and cartons as soon as possible. This helps to eliminate the possibility of tools, materials and equipment being hidden and carried off of the construction site.			

No.	Item	Yes	No	Further action needed
11	Are keys issued to authorised persons only and issue records maintained?			
12	Are spare keys secured in a location with limited access?			
13	Have all key control numbers been removed from the padlocks?			
INTERNAL THEFT				
14	Has a policy on employee theft been established and are employees/contractors aware of the policy? Information should be posted prominently.			
15	Is there a tool check-in and check-out system? • Record data on individuals responsible for specific tools. Include date, what was taken and by whom. • Secure tools stores at all times.			
SITE SECURITY				
16	Is there a security fence/boundary • Type of fence; Heras temporary fence/Closeboard/Chain-link/Steel-mesh/palisade/wall/other • The fence line should be clear of shrubbery, equipment, or buildings to eliminate possible hiding places. • Employees should either park their personal vehicles outside the fence or have a specifically designated parking area within the site to minimize the theft of tools, material and equipment.			
17	Is the fence inspected regularly? • Make sure that there are no holes or weak spots. • Check areas under the fence to ensure that offenders haven't gained entry underneath the fence			
18	Are "No Trespassing" signs displayed in a prominent place on the fencing or the perimeter of the construction site?			
19	Have gates been kept to a minimum? How many?______________________			
20	Are gates closed and secured at night and during weekends?			
21	Are there two sets of gates operated in an "airlock" system?			
22	Are drivers of unrecognized vehicles challenged and confirmation sought that they should be on site?			
23	Are manned guards used to check vehicles entering and leaving the construction site?			

No.	Item	Yes	No	Further action needed
24	Are there storage containers or fenced areas provided for tools, plant and equipment? • Heavy plant should be placed in front of storage shed doors to enhance security. • Doors of storage containers facing toward the perimeter of the construction site so that they are easily observed.			
25	Are vehicles locked and ignition keys removed?			
26	Are large items of plant, equipment and other machinery disabled? • Remove spark plugs or disconnect batteries • Install a hidden cut-out switch			
27	Are metal shields or screens utilized on windows to reduce vandalism?			
28	Are fuel supplies, including vehicle and plant fuel caps secured?			
29	Are blades and buckets of earth moving equipment dropped to the ground to make it difficult to move?			
30	Is equipment parked so that it is obvious if something is missing? Use designated or marked areas			
31	Are there tracking devices on large equipment and plant?			
32	Are there access control measures in place for contractors and visitors to site? Type of access control – Turnstiles/pass gates/biometric/PIN/Card or token			
33	Are there adequate control measures in place for the management and control of passes and tokens?			
CCTV				
34	**Has CCTV been installed on site?**			
35	Has an Operational Requirement (OR) for the CCTV been produced? • The OR should specify the areas to be covered by CCTV (Access Points, Fence Lines, Equipment Stores, Office areas) • The OR should specify the image type: • Monitor • Detect • Recognise • Identify			

No.	Item	Yes	No	Further action needed
36	Is it monitored and recorded? • CCTV should be monitored and recorded either on site or by a Remote Monitoring Station • CCTV should be recorded and the images retained for at least 31 days • Ensure CCTV is used in accordance with the Information Commissioner's Code of practice for CCTV (www.ico.gov.uk)			
37	Are Data Protection Act notices displayed?			
LIGHTING				
38	**Is there adequate lighting on the construction site(s)?** • Lighting should be illuminated to a minimum consistent with applicable local regulations and should be visible from the roads bordering the construction site. • Direct lighting toward the construction site to illuminate plant and buildings. • Lights triggered by motion detection or passive infrared sensor are recommended. • Consider the following location for lights: Access points, office complex, equipment storage area, materials storage area, area under construction.			
39	Are the lights checked regularly to ensure that they are working properly?			
ALARMS				
40	Is there an alarm system? • Type of alarm system- PIR/Active IR/Microwave other • Consider portable alarm systems that detect motion, activate lights and sound alarms. It is recommended that alarms sound locally at construction sites. • Consider an alarm that goes directly to a security monitoring centre that in turn notifies the local police. • Consider integration the alarm system into the CCTV system.			
MANNED GUARDING				
41	Is there a SIA licensed manned guarding company to providing either static, or mobile security presence at site? • The advantage is that they can be given access to patrol inside the job-site as well as the perimeter. They can also be given the responsibility for checking lighting and alarm systems on the construction site, as well as the integrity of fencing on a regular basis. • The use of dog patrols may be considered.			
42	Are there Assignment Instructions issued for the site? Examine Assignment Instructions to ensure duties reflect what is required to secure the site (patrols, checks of equipment, emergency procedures etc).			