ALLIANZ GLOBAL CORPORATE & SPECIALTY®

RISK BULLETIN

CONSTRUCTION SITE SECURITY

A Contractor's loss prevention guide

ALLIANZ RISK CONSULTING

INTRODUCTION

Providing and maintaining appropriate levels of site security benefits both the owner and contractors, as it will protect the site, reduce the potential for theft and restrict entry to only authorized personnel.

It is understood that security requirements can vary significantly from one project to another. For example, different security provisions will be required for a single inner city high-rise building compared to an infrastructure project, perhaps stretching many kilometers (miles) in rural areas. Additionally, security will be influenced by the local, legal, social and geographical exposures of the location.

The purpose of this document is to provide a general introduction and benchmark for the requirement of construction site security. It contains advice including best practice examples, assessment tools and checklists which may be used by the owner and contractors to assess security needs and provide mitigation strategies globally across all their construction sites.

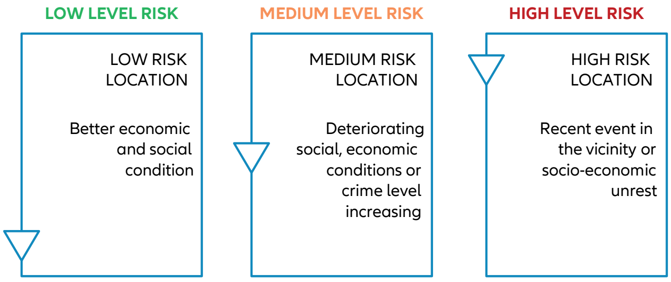
SECURITY ASSESSMENT PROCESS/ CONSULTATION WITH LOCAL ADMINISTRATION

Security risks vary according to the construction type and site location and can originate not only from the external population but also from the project's own workforce. The following are security assessment suggestions; however, recognize that each site will be unique, requiring specific and thoughtful consideration and planning.

Initial site security assessment is carried out by the owner or construction site management and should consider the following major factors:

- Project location: Exposures arising from neighboring properties and specific to urban or rural locations.
- Project type: Nature of the project (i.e. vertical or horizontal project) and value of equipment and materials utilized.
- Location Specific Exposures: Does the site location influence exposure to arson or intrusion? Socio-economic profile of locality, including crime rate and nature of crimes.
- Project Public Support: Is the project a benefit or an inconvenience to the surrounding public in the area? Does the project enjoy public support or is it perceived as a detriment and a likely target for vandalism, theft or trespass?

SOCIO-ECONOMIC IMPACT ON SITE RISK



LOW LEVEL RISK

LOW RISK LOCATION

Better economic and social condition

MEDIUM LEVEL RISK

MEDIUM RISK LOCATION

Deteriorating social, economic conditions or crime level increasing

HIGH LEVEL RISK

HIGH RISK LOCATION

Recent event in the vicinity or socio-economic unrest

AGCS_Insurance

agcs.allianz.com

This assessment should be periodically reviewed and revised to reflect changes such as, security risks, project boundaries, progress of work, construction methodology / sequence, logistics plan, etc.

The risk assessment process should be dynamic and encompass changes to internal and external conditions common throughout all phases of the project.

THREATS AND SECURITY MEASURES

Once the risk level and impact to the construction site is assessed, mitigation measures can be devised. The next sections detail various threats and mitigation measures highlighted in the following topics:

- Security related threats to construction sites
- Main steps to develop a site security plan
- Practical suggestions for addressing the overall security risks
- Various site mitigation methods for typical threat or loss source types
- Cyber security considerations for the construction site
- Emerging technologies and security requirements

SECURITY RELATED THREATS TO CONSTRUCTION SITES

- Theft of equipment and/or tools
- Theft of fuel
- Theft of materials from the site or off-site project storage areas
- Vandalism
- Arson
- Breaches of security into existing buildings or partially completed project areas.
- Robbery of or attacks on construction workers
- Reconnaissance of development to discover details of the in-process or completed project / building
- Trespassers: both accidental and intentional
- Cyber-attack or disabling closed circuit television (CCTV) security systems
- Protesters (either related to the site activity or simply for publicity)

MAIN STEPS TO DEVELOP A SITE SECURITY PLAN

- Carry out the security assessment of the project and consider the utilization of a third party security company if the expertise is not available "in house".
- Based on assessment, set the requirements for site security.
- Design the security system with consideration given to the inclusion of the following components, as warranted by the conditions:
  - Video
    Identify the locations where risks are concentrated and determine the camera types and quantity required.
  - Audio
    Alarms and provide verbal warning to intruders
  - Lighting
    Motion actuated lighting (white and infrared light)
  - Physical barriers
    Delay the intruder's site access using multiple fences and making the access indirect for places of intruder interest.
  - Response Mechanisms
    Devise an effective means to deter, delay and deal with the risks as soon as detected / identified / realized, such as, sirens, alarms, high beam lights, physical security on site to address as per local laws. If the residual risks are still too high, hire guards to carry out security duties.
- Periodic review of the security plan as the site changes (necessary to identify gaps in the security plan).
- Consider independent or third party security audits, especially for sensitive facilities.

PRACTICAL SUGGESTIONS FOR ADDRESSING OVERALL SECURITY RISKS

- Before the project commences create a site specific security plan based on the assessment of the security risks. Record and document this plan and have a written security policy.
- Liaise with local law enforcement agencies to assess the risks as envisaged by local municipal administration. If available, obtain advice from your own company's experts.
- Assign supervisory security responsibilities within the site/project management team, and encourage security awareness among all workers. Contact the local police and fire departments before starting a project to establish coordinated efforts. Establish contact with management of neighboring properties, and encourage them to report suspicious activities.
- Maintain a Security Risk register and periodically review the security plan and update registers as needed.

Solar Powered CCTV –especially useful where supplied power is unavailable

- Secure the site perimeter with appropriate fencing (as per risk assessment) as a first line of defense. Maintain a clear zone adjacent to fencing wherever practicable. Note that this clear zone may also benefit as a fire break.
- Illuminate the job site perimeter fence, high value storage areas, building entrances and the site offices to effectively deter trespass, theft and vandalism.
- Identify key assets and property onsite and then produce an inventory to track them regularly. Consider for high value items possible use of asset tagging and tracking systems.
- If appropriate, consider offsite storage and transit locations for mitigation against theft and vandalism.
- Where practical, secure all available high value materials and secure / immobilize vehicles and equipment. Consider installing hidden ignition disable switches to prevent theft.
- Control site access by establishing the minimum practical number of access points and monitor those entry points.
- Restrict site entry only to authorized personnel
- Provide guards at all entry points (personnel and vehicles)
- Consider limiting onsite vehicle access. Provide parking areas off site for employees and visitors.
- Ask employees and subcontractors to take personal responsibility for a secure site and engage them to immediately report any incidents of theft or vandalism.
- If appropriate, use a licensed and bonded security guard service to patrol the site both during and outside of working hours. It is suggested that guard rounds are digitally recorded to ensure they are actually being performed. Provide guards with an effective means of communication with local law enforcement agencies and project management 24 / 7.
- Periodically review the security plan with special attention to boundary changes and high risk areas as the project progress. Be aware of how changes to the project scope affect security.
- Consider installing a video monitoring system with advanced video analytics capability designed to detect and alert in the event of intrusion, vandalism, theft, fire and even water leak detection.
- Consider layered security to mitigate any gaps in the security system.

Review the above steps vigorously before and during extended suspension or slowdown of work due to holidays, weekends or planned and non-planned events (i.e. accidents investigations or natural catastrophe events, etc.)

VARIOUS SITE MITIGATION METHODS FOR TYPICAL THREAT OR LOSS SOURCE TYPES

This information can be used to define the scope of site security team / company

Site Risks	Risk Mitigation
Theft	Perimeter fencing suitable to project security risk Suitable anti-climb barrier walls or fencing, barbed wire fence, electrified, armed guards, etc. *Check local laws for compliance.*
	Illumination of fenced boundary
	CCTV / Night vision cameras Note that monitored CCTV cameras are always preferred to actively deter theft vs. passive CCTV systems which only record it happening. The use of a central station monitored video surveillance camera system is a best practice. The placement of such security cameras will vary depending upon jobsite conditions and size, but should cover the entire jobsite perimeter and select interior locations of the building. The surveillance system should be monitored by a listed or approved central station alarm monitoring service. The central station service should be instructed to call local police and management upon any intrusion or suspected intrusion. The use of a central station monitored security system which employs motion detection, sound detection, and/or other technologies is also a best practice.
	Intruder detection system – Infrared motion detection and local alarm/ remote alarm
	Security guards / patrolling / guard posts / security control / guard dogs (if applicable) / access control system
	Warning signs installed – indicating that CCTV and guards used
	Vehicle movement radar / global positioning system (GPS) vehicle tracking
	Worker tag in and out gates / biometric / face recognition – if allowed by local laws
	Programmed drones for site monitoring at random intervals – particularly useful for large areas – such as pipeline / road / railway infrastructure projects
	Worker screening / background check as allowed by local laws
	Locking and securing of all portable and particularly small size high value items
	Labor / workforce tracker & monitoring
	Time lapse photography (also useful for progress monitoring)
	Programmed computerized cameras to video record certain areas at the time of movement or incident only.
	Equipment tagging – appropriate for specific item and resources
Vandalism and arson	Adequate clearance maintained near site perimeter fence/boundary
	Entrance barriers and gates, including, where appropriate, high strength bollards to prevent unauthorized vehicle site entry
	Prohibition of storage of flammable & combustible materials near the project perimeter/boundary walls or fences
	Warning signs to discourage vandalism and arson (such as, No Trespassing – *violators will be prosecuted to the full extent of the law.)*
	Wireless fire detection systems
	IR and other types of motion sensors with remote CCTV monitoring & warning
	Security by design For example, avoid windows with ordinary glass panes. Consider using noncombustible, unbreakable / tougher material for cladding, such as poly-carbonate sheets or wired glass as an alternative to plain glass.
	Disable / Lock Mobile Construction Equipment Ensure equipment is not easily started and operated by unauthorized personnel or trespassers.

Site Risks	Risk Mitigation
Visitor Control	Maintain a visitor register and ensure the safe departure of visitors
	Issue temporary passes to document and track the entry of temporary workers and visitors
	Provide appropriate briefing for visitors as per site security procedures and requirements
	Escort and track visitors (provide tracker devices to them if they are unescorted)
	Deploy informative signage for the correct guidance of unescorted visitors
	Provide physical means for exclusion of visitors from active work areas.
Water Leak	Guard duties should include visual monitoring for a water release. An emergency after hours call list should be provided to on-site security personnel indicating who to contact 24 / 7 in the event of a water release. Security personal should be trained in water shutoff procedures in the event of a leak to minimize damage.
Fire	Guard duties should include knowing how to respond in the event of a fire and who to contact (fire department, project manager, etc.). Guards should know the location of fire extinguishers and be trained how to respond in the event of an incipient stage fire, including emergency notification of local authorities. Security personnel should be equipped with suitable communication devices (radio, wireless telephone, etc.)
Very cold weather	If freezing conditions are forecasted and heating is interrupted or the exterior of a building is opened for access or repair work, guards should be aware of the risk of pipe freezing and rupture and know who to notify to avoid or mitigate a potential loss.

CYBER SECURITY CONSIDERATIONS FOR THE CONSTRUCTION SITE

With the increasing reliance being placed on the role of Information Technology (IT) systems in all phases of construction, it is a vital that this digital information is adequately protected from malicious damage or theft by unauthorized persons.

- Make use of privileged account security and limit access on a need basis for each device connected to the network.
- All data should be encrypted; especially media taken offsite. If data is stolen but encrypted the hackers won't be able to use the data.
- All Internet Protocol (IP) CCTV cameras are susceptible to hacking since they are connected to the internet and no longer simply part of a hard wired, isolated system. Preferably, IP and night vision cameras should operate independently (air gapped) from rest of the project's IT system. Also, the security company should ensure that software security patches associated with the IP cameras are deployed promptly.
- Air gapping (islanding) should be implemented to prevent hackers from infiltrating and accessing all company data and specifically all computers installed on the project site. The simplistic approach would be to disable access to personal email accounts, social media and giving "read only access" to project information, drawings, and specifications.
- Install firewalls and establish a two level password access system to enable project team members to securely access project information.
- Limit the use of unnecessary data transfer and disable widespread use of USB and CD drives for laptops and office computers. File uploads from USB's, portable drives and FTP sites should be automatically scanned for malicious code / malware.
- All data systems should be protected by reliable and updated antivirus software.
- Sensitive project sites, where a data breach is critical, are advised to assess the robustness of security and IT systems through periodic external PEN (Penetration) testing conducted by third parties to identify potential weaknesses.

EMERGING TECHNOLOGIES AND SECURITY REQUIREMENTS

New technologies are being continually developed and are becoming more economical for use where it was not feasible some years ago. Construction management should be aware that although these new tools are useful and beneficial, sometimes they can be used for negative intentions and the risks posed by some technologies are changing rapidly.

Because of the complexity of emerging technologies and security, owners and contractors may want to consider hiring a professional turnkey security solutions provider to assess the project's evolving security needs and provide a holistic solution. Many companies provide security solutions specifically for construction.

Some of the emerging technologies to be considered when developing a security program are discussed in the following section of this document.

Drones

The benefit drones offer for some construction projects are well known. However, they may also pose different threats to civil engineering or construction projects.

For example, drones have been and can be used to breach the site's security and provide intruders with information facilitating later theft or collecting non-public project information. Drones have the potential to distract the equipment operators or interfere with critical lifting operations, or may damage equipment if the drone impacts critical / sensitive equipment.

If uninvited drones are observed, mitigation efforts should be taken to safeguard against any such possible threats, including deterrents and contacting local law enforcement to prevent such violations.

Asset Tagging by Electronic and Chemical/synthetic DNA systems

Electronic tagging is used to track the assets / equipment by scanning barcode labels attached to the assets or by using tags employing global positioning systems (GPS), blue tooth low energy (BLE) or radio-frequency identification (RFID) which broadcast their location.

Synthetic DNA has been used for tagging equipment and thieves during a robbery. This DNA marking system utilizes synthetic DNA which cannot be copied or analyzed by unauthorized parties. Signage alerting to the use of the system discourages theft and the DNA marker helps the local authorities to recognize and identify the stolen or illegally acquired items recovered from the criminals.

Microdots

Microdots are very tiny discs that are held in an adhesive solution. A small amount of the solution is applied with a brush to the surface of the equipment and the item is tagged. Each microdot carries a unique code and database contact telephone number that has been printed on them. These microdots can just about be seen by the naked eye, but the detail printed on them can only be viewed under a microscope (hand held, pen sized, scopes with lights can be supplied). The unique codes on the discs can then be checked against a database to identify the owner. The solution holding the microdots will also have a dye which is visible under ultra violet light.

Audio addressable CCTV systems

Video surveillance systems with active monitoring (often at an offsite monitoring facility) can be used with live audio to warn the intruders that their activities are monitored and authorities will respond if the intruder does not vacate the site.

High Definition Cameras

High definition / high resolution cameras can be installed to take time lapse photographs or continual video when a problem is detected at a site location and can be viewed remotely. Remote camera stations can also be used to transmit the site videos to security centers on a continuous basis, day or night.

Smart phone Apps

Motion detectors and alarms can be connected to mobile devices to provide warning and facilitate a rapid response if unusual activity occurs at the site.

Allianz has prepared Installed Building Services and Equipment - A Contractor's Loss Prevention Guide, which addresses installed equipment losses (with theft being one loss mechanism) which result in a significant portion of builder's risk claims and protection measures which can be taken. Please request this guide from your Allianz Risk Consultant.

Builder's risk insurance experience has shown that proper site security and planning are imperative to preventing theft, vandalism, arson, public safety, fire and leak detection and proactive hazard identification.

It becomes evident when investigating many losses, that a construction site security strategy and emphasis would have been a wise investment saving far more than it costs to implement.

Losses attributable to the lack of - or inadequacy of - construction site security may take many forms, but in all cases can result in delays in project completion, lost profits, reputational damage, rework and even injury to the public. Our construction experience indicates that appropriate construction site security, considering the points discussed in this document, is imperative to the prevention of construction related losses.

For more information contact:

Jay M. Siegel, P.E., CPCU
Sr. Team Leader, Engineering, Construction All Risks
Office Phone: +1.770.558.6844
jay.siegel@agcs.allianz.com

agcs.allianz.com

Design: AGCS Graphic Design Centre

This article provides general information and recommendations that may apply to many different situations. Any recommendations described in this article are not intended to be specific to your unique situation. Consult with your specialists to determine how and whether the information in this article might guide you in developing specific plans or procedures. This article does not substitute for legal advice, which should come from your own counsel. Any references to vendors or third-party websites are provided solely as a convenience to you and not as an endorsement by Allianz Global Corporate & Specialty SE of the vendors or the content of such third-party websites. Allianz Global Corporate & Specialty SE is not responsible for the goods or services provided by vendors or the content of such third-party sites and does not make any representations regarding the goods or services provided by vendors, or the content or accuracy of materials on such third-party websites. If you decide to use a vendor or access third-party websites, you do so at your own risk. Any descriptions of coverage are abbreviated and are subject to the terms, conditions and exclusions of the actual policy, which forms the contract between the insured and the insurance company. Availability of coverages, credits and options may vary by state or region.