INSIGHT PAPER

BEYOND THE FENCE LINE

Protecting Corporate Assets in Austere Environments

CORE ASSESSMENT

Corporate physical security is frequently strongest at the point of detection and weakest immediately afterwards. Companies invest in fences, guards, cameras and alarms, yet often cannot answer the operational questions that follow: who verifies the incident, who is told, who decides, who acts, who calls external assistance, and what the organisation does while that assistance is still en route. In austere environments, where response times may be extended and support relationships uncertain, this gap can turn a manageable event into an operational failure. Effective asset protection therefore has to connect criticality, detection, decision, response, continuity and recovery as one corporate system.

ADG CONSULT NZ

September 2026

Executive Summary

Corporate physical security is frequently strongest at the point of detection and weakest immediately afterwards. Companies invest in fencing, guards, access control, closed-circuit television, alarms and tracking systems, but far fewer can explain with the same confidence what happens after a guard sees something unusual, a camera operator verifies an intrusion, or an employee reports a developing threat. The critical gap is often not the absence of security equipment. It is the absence of a rehearsed decision and response architecture.

This problem becomes more serious in austere operating environments. The nearest police unit may be distant, emergency services may have limited resources, communications may be unreliable, and the organisation may depend heavily on contractors or locally recruited personnel. A national emergency number may exist, yet the company may have no established relationship with the local police unit that would actually respond, no clear understanding of jurisdiction, and no realistic estimate of how long authorised assistance will take to arrive. During that period, the company remains responsible for its people, critical assets and operating decisions.

The paper therefore argues that corporate asset protection should be designed as a continuous chain from criticality through detection, decision, response, continuity and recovery. The decisive questions are practical. Who sees the problem? Who verifies it? Who is told? Who decides what happens next? What is the guard authorised to do? What do employees do? When does site management become involved? Who calls the police, medical service or other authority? Are those relationships already in place, and what does the company do while it waits? These questions should be answered before an incident rather than during one.

The paper also makes a broader business argument. The purpose of physical security is not to make a facility impossible to penetrate. It is to prevent a foreseeable security event from becoming a business failure. That requires management to identify what the organisation genuinely cannot afford to lose, concentrate protection on those dependencies, establish realistic response arrangements, rehearse them, and retain the ability to continue operating when prevention ultimately fails.

Protection Is Only as Good as the Response

A security system can perform exactly as designed and still fail the business. A camera records the intruder. The perimeter alarm activates. The control room receives the alert. A guard confirms forced entry. Every technical element may be functioning, yet if nobody knows who has authority to call the police, whether the guard should approach, who tells the site manager, or what employees are expected to do while external support is on the way, detection has merely identified the point at which uncertainty begins.

This is the response gap. It is commonly hidden because physical-security reviews are easier to conduct around things that can be seen and counted. Fence condition, lighting coverage, guard numbers, camera placement and access-control hardware are tangible. The quality of a decision chain is harder to inspect. It requires asking people to explain what they would actually do and then testing whether the contact numbers, authority, communications and external relationships on which the plan depends are real.

The principle is consistent with recognised protective-security guidance. The United Kingdom National Protective Security Authority (NPSA) links deterrence, detection, delay, mitigation and response as complementary functions and explicitly treats detection as the mechanism that should initiate an appropriate response.[3] The important corporate implication is that an alarm, camera or guard post should never be assessed independently of the action it is expected to trigger.

OBSERVATION: Do not confuse having a telephone number with having a response arrangement. A national emergency number may allow a company to request help, but it does not tell management which unit will respond, whether that unit knows the facility, who can be reached after hours, how long deployment will take, or what the company must do in the meantime.

The Asset Is the Capability

Traditional physical security focuses naturally on tangible property: buildings, machinery, warehouses, vehicles, equipment and inventory. Those assets matter, but a company operating in a difficult environment depends on a much wider system. Fuel supply, power generation, communications, critical spares, access routes, specialist personnel, data, permits, transport capacity and key suppliers can each become operational single points of failure.

The distinction between financial value and operational criticality is especially important. A low-cost electronic component may support equipment worth several million dollars. If that component is stolen and a replacement must be imported, the direct loss may be minor while the cost of delayed production, idle personnel or suspended field activity is substantial. A company that protects assets according only to replacement cost can therefore spend heavily while leaving its most important dependencies exposed.

ISO 31000 places risk treatment within the broader objective of creating and protecting organisational value, while the ASIS Enterprise Security Risk Management approach emphasises partnership between security professionals and asset owners to identify and prioritise the assets and risks that matter to the organisation.[1][8] For physical security, the practical test is straightforward: what can the business not afford to lose, how long can it function without it, and what response or redundancy is required if protection fails?

Austere Does Not Necessarily Mean Hostile

An austere environment does not need to be a conflict zone. A company can face significant physical-security exposure in an area with relatively low levels of violence if infrastructure is unreliable, government response is limited, supply chains are long, communications are fragile, or specialised commercial support is difficult to obtain. These conditions magnify small failures because the operating system has less capacity to absorb them.

A generator failure at a city office may be an inconvenience. At a remote camp it can affect lighting, communications, water, refrigeration, access control and operational equipment at the same time. A stolen vehicle in a developed market may be replaced quickly; the loss of a specialised four-wheel-drive vehicle supporting a distant project can interrupt movements for days or weeks. The severity of the event therefore lies not only in what happened, but in the operating environment around it.

This is why physical protection and business continuity should be connected from the outset. ISO 22301 treats continuity as the organisational capability to prepare for, respond to and recover from disruptive incidents.[2] In remote operations, the same logic should inform security planning: protection should reduce the likelihood and consequence of loss, while continuity arrangements ensure that the organisation can absorb the failures it cannot economically prevent.

The Perimeter Fallacy

Visible security is attractive because it is easy to inspect. A wall exists or it does not. A guard is on post or absent. A camera produces an image or it does not. This can encourage an organisation to treat the perimeter as the security system rather than one layer within it. A well-fenced facility may still be vulnerable because contractors move without supervision, access cards are shared, keys are uncontrolled, guards bypass procedures for familiar personnel, or the monitoring centre has no effective response to what it sees.

The perimeter can therefore perform perfectly while the business remains exposed. Effective asset protection requires layers that deter, detect, delay, support decision-making, enable a response and reduce the consequence of failure. The objective is not necessarily to make the outer boundary stronger. It is to ensure that no single control failure immediately exposes a critical asset and that each layer is connected to a realistic action.

NPSA guidance applies this logic beyond the perimeter, at the perimeter, within the site, at the building and at the asset itself. It also stresses that response requirements should be determined for the full range of relevant threats and that response plans should be exercised with internal and external stakeholders where appropriate.[3][4] This is a useful discipline for companies because it prevents physical-security investment from becoming a collection of disconnected measures.

The Response Gap

The response gap becomes visible when a simple scenario is pushed beyond its first sentence. A guard identifies an intruder entering the site. The initial answer is often that the guard calls the supervisor, the supervisor calls the site manager, and somebody calls the police. The arrangement sounds plausible until the questions become specific. Which supervisor? On what number? What happens if that person does not answer? Can the guard call the police directly? Which police unit has jurisdiction? Does it know the location? Who has authority to close the site, stop vehicle movements or move employees to a safer area?

The same problem exists in urban environments. A recently dismissed employee arrives at reception and becomes aggressive. Building security, the corporate security team, Human Resources and management may all have an interest, but unless the roles have been decided beforehand the organisation can lose time determining who actually controls the response. Several people may issue competing directions, or everyone may wait for someone else to make the decision.

ProtectUK guidance on incident management highlights command, control, coordination and communication as essential components of managing the consequences of an incident.[6] For the corporate site, these concepts do not need to become complicated. Someone must own the incident, someone must have the authority to act, and everyone else must understand when responsibility moves from a guard or supervisor to site management and, if necessary, to a country or corporate crisis-management function.

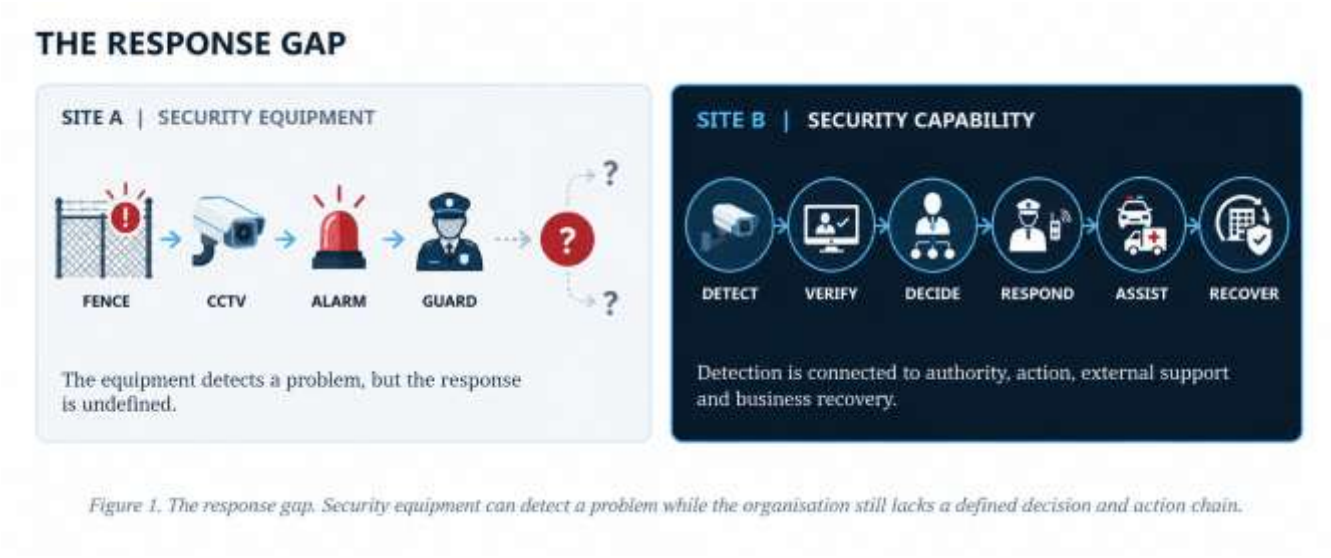

Figure 1. The response gap. Security equipment can detect a problem while the organisation still lacks a defined decision and action chain.

The First Five Minutes Matter

The initial response to a security event is frequently undertaken by ordinary people rather than senior managers. A guard, receptionist, driver, warehouse employee or control-room operator may have limited information and no specialist authority, yet the decisions made in the first few minutes can determine whether an incident remains manageable. The organisation should therefore decide in advance what the first person is expected to do, what that person is explicitly not expected to do, and how the incident is transferred to the next level of authority.

The instructions do not need to be complex. The appropriate action may be to observe from a safe position, withdraw, raise an alarm, call a defined number, close a gate, stop a vehicle movement, move staff away from a location or avoid intervention. What matters is that the first person who identifies the problem is not also required to invent the emergency response.

NPSA control-room guidance stresses the importance of clear communications between security officers, control-room staff and response personnel, including clarity over who should be contacted during an incident and what backup procedures apply if the primary communications system fails.[5] In practical terms, the first five minutes should be designed as deliberately as the physical barrier that triggered the alarm.

What Does the Guard Actually Do?

Security guards are often described as the first line of defence, but their most important corporate functions may be detection, verification, communication and controlled response. A guard who observes suspicious activity needs to know whether the correct action is to approach, remain under cover, call the control room, close the gate, stop vehicle movements, request another guard, contact police, or simply continue observation while the event is assessed.

These decisions should not be left to individual instinct. Sending a lone guard to investigate an alarm at a dark warehouse, for example, may create greater risk than the property loss the company is trying to prevent. The guard may be expected to verify from a safe position, protect access, report accurate information and support authorised responders rather than confront unknown intruders. The exact role will depend on local law, training, contractual arrangements and the threat environment, but ambiguity should be minimised.

Guard orders should therefore describe more than routine post duties. They should establish escalation thresholds, communications procedures, immediate protective actions and the point at which the guard's role ends and management or public-authority responsibility begins. Contracted guard forces should be included in exercises because a written contract is not evidence that both the contractor and client have the same understanding of who calls whom during an emergency.

Staff Are Part of the Response System

Most employees are not security professionals and should not be expected to become them. They do, however, form part of the response system. A receptionist needs to know how to raise an alarm without escalating an aggressive encounter. A warehouse employee who discovers tampering needs to know whether to investigate or withdraw. A driver approaching a facility during a demonstration needs to know whether to continue, hold at a pre-arranged location or divert elsewhere.

The instructions must be simple enough to use under pressure and realistic enough to match the way people actually work. A plan that requires employees to call a manager who is routinely unavailable is not operational. A procedure that relies on an emergency radio that staff have never used will fail when it is needed. A designated assembly area is of little value if the threat itself makes that area unsafe.

Training should therefore concentrate on a small number of actions: how to raise the alarm, where authoritative instructions will come from, what broad protective actions may be required and what employees should avoid doing. The purpose is not to create a complicated security culture. It is to ensure that the organisation does not add confusion to an already uncertain event.

Who Is in Charge?

Security incidents cross organisational boundaries quickly. An event at the gate can involve security, operations, Human Resources, health and safety, legal advisers, communications staff and senior management within minutes. Without predetermined authority, several functions may begin directing the response at the same time or, just as dangerously, everyone may wait for another department to take control.

A simple command structure is usually sufficient. The guard or control room owns detection and initial reporting. A security supervisor may coordinate immediate protective measures. A site manager may assume operational command. A country manager or crisis-management team may take responsibility when consequences exceed the site. The names will differ between organisations; the important issue is that participants understand when the transfer occurs and what powers accompany it.

The practical questions should be written down. Who can stop operations? Who can suspend access? Who can order employees to shelter, evacuate or relocate? Who contacts public authorities? Who communicates with the client? Who speaks to employees and, if necessary, their families? Who maintains the incident log? Who decides that the site can return to normal? These decisions are easier to make calmly in advance than under pressure during a developing incident.

The Call Tree Must Be Real

Many companies have emergency contact lists. Far fewer have demonstrated that those contacts form a functioning response network. A police emergency number, hospital switchboard, local authority contact and security manager may all be listed in a plan, but the existence of a number does not establish who will answer, whether the responder understands the facility, whether the organisation has the authority to request a particular form of assistance, or how long that assistance will take to arrive.

The problem is especially acute at remote or temporary facilities. A national dispatcher may be unfamiliar with the project. The site may be known locally by a different name. Digital mapping may identify the wrong entrance. The nearest police station may not be the unit responsible for response. Language differences can consume time. A responder may reach a locked gate that has no procedure for emergency access. None of these are unusual circumstances; they are foreseeable friction points that should be resolved before the event.

CISA guidance for temporary facilities recommends coordinating emergency action plans with local law enforcement and first responders, particularly where responders may not be familiar with the facility or its current use, and exercising those arrangements where possible.[7] The same principle is highly relevant to remote corporate operations. The company should know which organisation has jurisdiction, maintain more than one contact where appropriate, verify after-hours arrangements and ensure that external responders understand how to find and enter the facility.

Response Time Is a Security Control

One question should appear in every serious physical-security assessment: how long before authorised assistance actually arrives? The relevant figure is not the theoretical service standard or the distance shown on a map. It is the realistic time from a verified request for assistance to the arrival of a capable responder under the conditions in which the company operates.

The answer changes the entire security design. If competent assistance reliably arrives within minutes, the company's own response may focus on detection, communication, protection of personnel and preservation of the scene. If assistance is likely to take an hour, the site must be capable of managing that hour. If response may take several hours, management must consider how the facility communicates, controls access, protects employees, maintains essential services and adjusts operations during an extended period of isolation.

This does not mean creating a private police force. It means acknowledging the response window. Physical delay measures, internal safe areas, communications redundancy, authority to stop movements and continuity arrangements all need to be proportionate to the period before effective assistance becomes available. NPSA guidance explicitly recommends considering the potential length of response times when exercising response plans.[4]

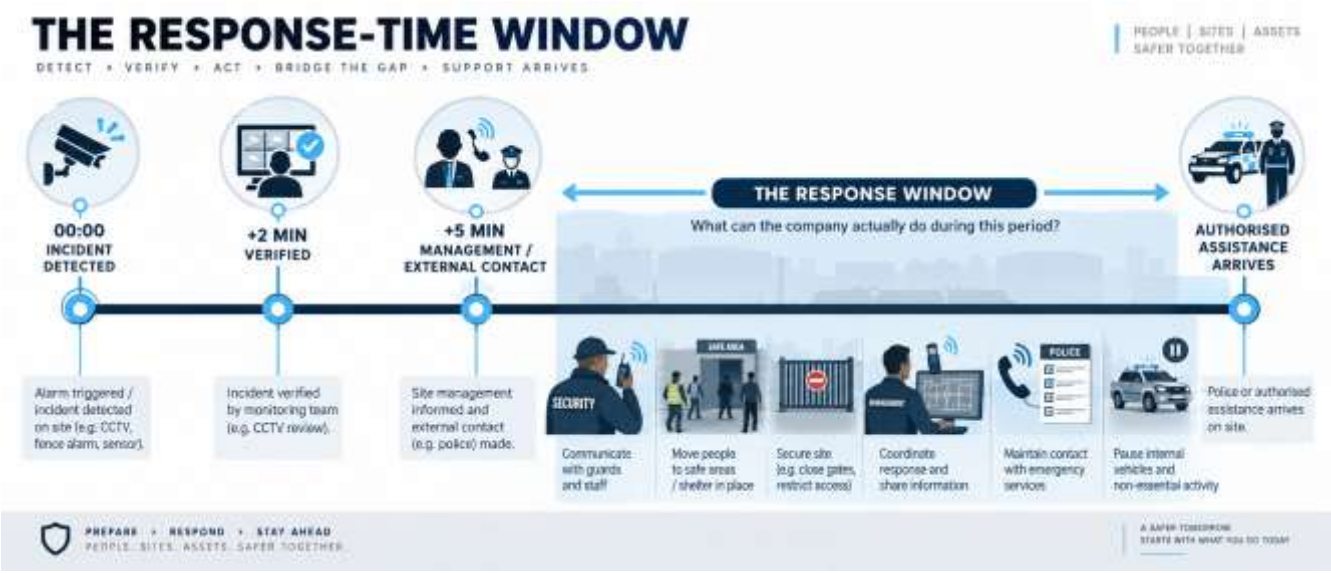

Figure 2. The response-time window. The key planning question is what the company can legitimately and safely do between detection and the arrival of authorised external assistance.

Build Relationships Before You Need Them

Some of the most valuable protective-security measures never appear on a capital-expenditure request. A facility manager who has met the local police commander possesses something that cannot be created at 02:00 during an emergency. A security manager who has confirmed which hospital will accept an injured employee has removed uncertainty. A project that has discussed access routes and site hazards with responders has eliminated another predictable delay.

These relationships should not depend entirely on one experienced individual. The security manager may know the police, hospital, community leaders and neighbouring companies, but a system that works only when that person answers the telephone has created another single point of failure. Important external relationships should be institutionalised through documented contacts, deputies, periodic confirmation and appropriate management visibility.

The same principle applies to local communities and neighbouring businesses. Community engagement should not be reduced to a security technique, but surrounding communities inevitably influence the operating environment. They see vehicle patterns, employment changes and unusual activity around the facility. Constructive relationships can provide early warning and reduce friction, while poorly handled land, procurement, employment or compensation disputes can turn community concern into a physical-security problem at the gate.

Insiders, Contractors and the Extended Perimeter

The organisation's security perimeter extends through everyone who legitimately enters the site or supports the operation. Employees, contractors, drivers, cleaners, maintenance personnel, suppliers and guards accumulate detailed knowledge of routines, weak points and critical assets. Most will never misuse that knowledge, but insider risk does not require malicious intent. Access cards are shared for convenience, doors are left unsecured, sensitive information is discussed casually, photographs are posted online and contractors enter areas that have little connection to their task.

The solution is not to treat the workforce as a threat. It is to design access and reporting arrangements that do not rely solely on trust. Access should match operational need, critical assets should receive additional control, credentials should be withdrawn when no longer required, and unusual activity should have a clear reporting route. Equally, a company should know how contractor access is supervised and what happens when a contractor identifies or becomes involved in an incident.

Outsourcing can also create response ambiguity. A monitoring company may believe the guarding contractor will call the police. The guard company may believe the client must authorise the call. The client may assume both contractors have already acted. These are not equipment failures. They are interface failures, and they should be identified through contract review and exercise rather than during a burglary, protest or violent incident.

The Supply Chain May Be the Real Perimeter

Important corporate assets spend significant periods outside the protected facility. Fuel travels on public roads. Equipment passes through ports, warehouses and temporary storage areas. Spare parts move through multiple intermediaries. Employees transit airports, hotels and staging locations. Protecting the final destination therefore addresses only part of the exposure.

Fuel illustrates the problem particularly well. A company may have strong controls around a fuel point while losses occur during transportation, transfer, delivery or reconciliation. Repeated small losses can become normalised because no single event appears sufficiently serious to trigger management attention. The same pattern can affect construction materials, spare parts, vehicle components and other consumables.

Asset protection should therefore follow the asset through dispatch, transportation, receipt, storage, issue and reconciliation. Just as importantly, discrepancies should trigger a defined response. Discovering that stock is missing is detection. Who investigates, who is notified, whether access changes, how evidence is preserved and when management becomes involved determine whether the control creates any deterrent or business value.

Technology Does Not Shorten the Response by Itself

Modern technology can provide excellent remote monitoring. Cameras, electronic access control, analytics, vehicle telematics, geofencing, sensors, satellite communications and centralised alarm platforms can reduce the time required to detect abnormal activity. They cannot, by themselves, make an authorised responder arrive sooner or make a manager decide faster.

Every technical security measure should therefore be tested against the action it is supposed to produce. Who receives the alarm? Who verifies it? What level of confidence is required before escalation? What local resource can actually respond? What happens at night? What happens if the communications network fails? Who maintains the equipment, and are replacement parts available? A camera that records a theft but has no timely response is primarily an investigative tool, not an effective intervention capability.

Remote technology can even widen the response gap if management confuses visibility with control. A control centre 1,000 kilometres away may see an intrusion instantly while nobody capable of intervention can reach the site for an hour. The technology has improved awareness but not necessarily protection. The response architecture must therefore be designed at the same time as the technology.

From Detection to Recovery

A mature security system assumes that some protective measures will eventually fail. A determined criminal may defeat a lock, an employee may abuse legitimate access, a road may close, communications may fail, or a supplier may stop operating. The relevant management question then becomes whether the business can absorb the event without losing a critical capability.

Recovery begins during the response. A warehouse may become a crime scene, a facility may remain inaccessible, equipment may be damaged, employees may be reluctant to return, or public authorities may retain vehicles and records as evidence. Security, operations and business-continuity functions should therefore work in parallel rather than waiting for the immediate incident to end before considering how the business will continue.

Sometimes the most effective security investment is not another barrier. Holding a critical spare locally, establishing a secondary communications path, identifying an alternative supplier or distributing critical inventory between locations may reduce business risk more effectively than additional perimeter expenditure. Security resources are finite, and the objective is not to prevent every possible loss. It is to preserve the organisation's critical operating capability.

Figure 3. The corporate asset protection chain. The central design problem is connecting detection to decision and response, then ensuring continuity and recovery if protection fails.

Measure Security in Business Terms

Security programmes often report what is easiest to count: guards, patrols, cameras, visitors screened and incidents recorded. These figures describe activity but do not necessarily show whether the organisation can protect its operating capability. A stronger corporate approach measures the time from detection to verification, from verification to management notification, from notification to protective action and from the request for assistance to effective external intervention.

Management should also examine downtime caused by security events, repeated losses, the availability of critical systems, the time needed to restore normal operations and the number of unresolved single points of failure. These measures connect security to production, service delivery, project schedule and financial consequence. They also make it easier to compare alternative investments. A new camera may be valuable, but a tested communications backup or a spare critical component may produce greater resilience.

This approach changes the conversation from how much security the organisation owns to what capability it actually possesses. Instead of asking how many guards are required, management can ask what response capability is required. Instead of asking how many cameras should be installed, it can ask what needs to be detected and what action the detection must trigger. Instead of asking whether the police number is posted, it can ask how quickly authorised assistance can realistically reach the site.

The Questions Management Should Be Asking

Senior executives do not need to become physical-security specialists, but they should be able to test whether the security system is real. A useful starting point is to ask a site manager what happens if something occurs at the gate tonight. Who takes charge? Who does the guard call? What does the employee do? Who informs management? Who contacts police or other authorised assistance? Which unit will actually respond? Have company representatives met them, and do they know where the facility is?

The next questions concern time and authority. How long will help take to arrive? What can the company legitimately do during that period? Who can suspend access, stop operations or divert incoming vehicles? What happens if primary communications fail? Where do personnel move if the normal safe area is compromised? Who can restart operations? If those questions cannot be answered clearly, the organisation has identified a security vulnerability even if the last physical inspection found every fence panel and camera in good condition.

The final question should address resilience: what happens if the response does not prevent the loss? If the answer is that the operation stops because one component, supplier, vehicle, communications link or individual has become unavailable, the company should treat that dependency as a business risk rather than assuming that physical security alone can eliminate it.

Beyond the Fence Line

Corporate physical security in austere environments is not primarily about constructing stronger barriers. It is about creating a functioning protective system around the business capabilities that matter most. The system begins with criticality, uses layered physical and procedural controls to deter and detect, and then connects detection to a clear decision chain. Guards must know what they are authorised to do. Employees must know how to raise the alarm and how to protect themselves. Managers must know when they assume control and what authority they possess.

External response arrangements are equally important. The company should understand who will actually respond, how those people will be contacted, what they know about the facility and how long they will realistically take to arrive. Relationships should exist before the emergency. Communications should have alternatives. Response procedures should be exercised, and the exercise should test the telephone numbers, authority and relationships rather than simply the written plan.

Finally, the organisation must be capable of continuing and recovering when protection does not work. That may require redundant equipment, alternative suppliers, critical spares, secondary communications or temporary operating arrangements. A secure facility can still support a fragile business if the loss of one asset stops the operation.

The most useful test of a corporate security system is therefore not whether it can prevent or detect every incident. It is whether the organisation knows what it will do when prevention fails and detection succeeds. A guard who identifies a threat has done his job. What happens in the next five minutes reveals whether the company has done its.

Appendix A – Tabletop Exercise One: Something Outside the Fence

This exercise tests the response arrangements of a remote corporate operating site when suspicious activity develops outside the perimeter and gradually escalates. It is suitable for an energy project, mining operation, construction camp, seismic base, remote warehouse or similar facility. The objective is not to test tactical expertise. It is to expose uncertainty surrounding guard actions, verification, management authority, employee protection, communications, external assistance and the period before authorised support arrives.

Directing Staff should release the injects progressively and should not provide participants with the complete scenario in advance. Participants should use the procedures, telephone numbers, communications systems and relationships that genuinely exist. Statements such as 'we would call security' or 'we would contact the police' should be challenged until the participant identifies exactly who would be contacted, by what method, what that person is expected to do and what happens if the primary contact fails.

Starting Situation

The facility accommodates approximately 100 personnel and is about 45 minutes by road from the nearest significant town. Local police have jurisdiction but no permanent presence at the site. The company has a perimeter fence, controlled entrance, guard force, CCTV, external lighting and radio communications. Normal operations are continuing when the exercise begins at 21:40.

Inject One – Observation

A perimeter guard reports that two motorcycles have stopped approximately 150 metres outside the facility. Three individuals are standing nearby. They are not attempting to enter the site, but one appears to be watching the entrance and another is using a mobile telephone.

PARTICIPANT QUESTIONS: What does the guard do immediately, and is the guard expected to approach? Who is notified and who verifies the report? Is CCTV reviewed and by whom? At what point is the site manager informed? Does the situation meet a threshold for police notification, are vehicle movements changed, and what information is recorded?

DIRECTING STAFF NOTES: The objective is to determine whether the guard has a clear instruction for suspicious activity rather than a general requirement to remain vigilant. Challenge vague responses. If participants say the guard will notify security, ask which person. If CCTV will be checked, establish who is actually on duty to do so. If police notification is proposed, ask who has authority to make that call. The exercise should distinguish observation, verification, escalation and intervention.

SUGGESTED RESPONSE: The guard should normally maintain observation from a protected position rather than leave the facility to investigate. The report should move immediately through the defined security channel and be verified through CCTV or another observation point where available. The event should be logged and the duty manager informed according to established criteria. Non-essential departures may be delayed while the situation is assessed. The key outcome is that one person clearly owns the developing incident and everyone understands the threshold for further escalation.

Inject Two – Escalation

At 21:52 another vehicle arrives and two additional individuals get out. One of the original individuals moves approximately 50 metres closer to the perimeter and appears to photograph the entrance. A company vehicle carrying four employees is due to arrive within ten minutes.

PARTICIPANT QUESTIONS: Who now owns the incident and does the response level change? Who contacts the approaching vehicle and where should it go? Are employees inside the site told anything? Should access or departures be suspended? If police are contacted, which unit is called, what number is used, does the company have a named contact and what information is passed?

DIRECTING STAFF NOTES: Pay particular attention to the approaching company vehicle. Exercises often concentrate on people already inside the facility while forgetting personnel moving toward it. Determine whether there is a designated holding point or diversion location. If police are called, require participants to identify the actual number and the unit expected to respond rather than simply saying that police will be notified.

SUGGESTED RESPONSE: The site manager or designated incident manager should assume control. Incoming personnel should be warned before reaching the site and sent to a pre-identified safe holding location. Unnecessary movement through the gate should stop. The guard force should maintain observation without creating an avoidable confrontation outside the perimeter. Police or other authorised support should be contacted through the established arrangement, and management should verify that primary and backup communications are functioning.

Inject Three – The Response Gap

Police acknowledge the call but advise that the closest available patrol is dealing with another incident. Estimated arrival time is between 45 and 60 minutes. At 22:03 external lighting on one side of the compound suddenly fails. The cause is unknown.

PARTICIPANT QUESTIONS: What does the company do for the next hour? Who can change the site's operating posture? Are employees moved and, if so, where? Are operations suspended? What happens at the gate and to additional incoming vehicles? Is anybody sent outside to investigate the lighting failure? Who keeps the police updated and who informs country management?

DIRECTING STAFF NOTES: This is the central learning point. Do not allow participants to focus only on when police will arrive. The question is what the organisation can safely and lawfully do during the response window. If somebody proposes sending a technician outside to inspect the lighting, ask whether the task is essential while suspicious persons remain nearby. If sheltering is proposed, ask whether the selected location genuinely protects personnel from the identified threat.

SUGGESTED RESPONSE: The site should move to a predefined heightened-security posture. Non-essential external movement should cease and personnel should remain in designated protected areas appropriate to the local threat. The failed lighting should not be investigated externally until conditions permit. Alternative lighting or observation should be used if available. Police should receive significant updates and country or corporate management should receive an initial situation report. The site should plan for a response period longer than the first estimate rather than assuming assistance will arrive at the earliest stated time.

Inject Four – Communications Failure

At 22:14 the site's primary cellular network fails. Internal radio communications still work, but the company does not know whether the outage is connected to the developing incident.

PARTICIPANT QUESTIONS: What is the backup communication method, who has access to it and when was it last tested? Can police and senior management still be contacted? Can incoming vehicles still be warned? If communications capacity is limited, who decides which messages receive priority?

DIRECTING STAFF NOTES: The purpose is to determine whether communications redundancy exists operationally rather than only on paper. If participants refer to a satellite telephone, establish where it is kept, whether it is charged, who knows how to use it and whether the police or corporate contacts can actually be reached through it.

SUGGESTED RESPONSE: The site should transition immediately to the established secondary communications method. Priority should be given to emergency-service contact, incident command and warning personnel travelling toward the facility. Internal radio traffic should be controlled so that the operational channel remains available. The communications failure should reinforce the protective posture until its cause and duration are understood.

Exercise End State and Debrief

Police arrive at 22:48. The individuals outside the facility leave several minutes before the patrol reaches the location and no attempt is made to enter the site. The exercise should end by asking what the organisation assumed it could do at 21:40 but discovered during the scenario that it could not actually do. Actions should be assigned to named owners with completion dates, with particular attention to police liaison, alternate communications, diversion locations, guard authority and the ability of management to control the site during a prolonged response window.

Appendix B – Tabletop Exercise Two: The Alarm Worked

This exercise tests whether an organisation can translate successful technical detection into effective intervention and continuity. It is suitable for a warehouse, equipment yard, logistics facility, office compound or regional support base. The scenario deliberately demonstrates that the alarm, monitoring system and guards can all work as designed while the overall protective system still fails because response time, responsibilities and business criticality were not considered together.

Starting Situation

A regional warehouse contains specialist equipment, vehicle components and critical spare parts supporting several projects. Total replacement value is approximately USD 3 million, but several individual components have long international replacement lead times. The warehouse is protected by perimeter fencing, CCTV, intrusion detection and contracted guarding and is normally unoccupied between 22:00 and 05:30. The exercise begins at 02:15.

Inject One – Alarm Activation

The contracted monitoring centre receives an intrusion alarm from the rear perimeter. The operator attempts to view the relevant CCTV camera but the image is partially obscured. The operator calls the contracted guard supervisor.

PARTICIPANT QUESTIONS: What does the monitoring operator do next? Who does the guard supervisor inform? Is a guard sent to investigate, how many personnel respond and what are they expected to do? Is the company informed immediately, who receives the call at 02:15 and what happens if that person does not answer?

DIRECTING STAFF NOTES: This inject is intended to expose assumptions created by outsourced security arrangements. Determine whether the monitoring provider and guarding company share the same escalation procedure and whether the contract specifies when the client must be informed. Do not allow 'investigate' to remain undefined; require participants to describe the responding guard's task and limits.

SUGGESTED RESPONSE: The monitoring centre should follow a predetermined verification procedure and the corporate duty contact should be notified according to agreed thresholds rather than only after a crime is confirmed. Responding guards should understand that their primary role is observation, verification, reporting and protection of personnel. Where the threat is uncertain, the company should avoid sending a lone employee toward a potentially hostile situation unless that response has been specifically trained, authorised and assessed.

Inject Two – Forced Entry Confirmed

At 02:31 the responding guard reports damage to the rear perimeter and an open warehouse access door. He can hear movement inside the building.

PARTICIPANT QUESTIONS: Does the guard enter the building? Who calls police and is that responsibility assigned to the guard company or the corporate duty manager? Who assumes control of the incident? Is another security resource dispatched? Should the warehouse manager or other managers travel to the site?

DIRECTING STAFF NOTES: Participants may instinctively want somebody to enter the warehouse to protect company property. Force consideration of personal safety, legal authority, training and role. This is also the point at which unclear contractual assumptions often become visible. The guarding company may believe the client must call police while the client believes the guarding company has already done so.

SUGGESTED RESPONSE: The guard should remain at a safe observation position, report developments and avoid entering a building containing potentially hostile individuals unless the organisation's lawful security arrangements specifically require and support that action. Police should be contacted immediately through a predetermined responsibility. The company duty manager should be informed, access to the area should be controlled and significant events and decisions should begin to be recorded.

Inject Three – Police Response

Police acknowledge the incident but advise that the estimated response time is approximately 35 minutes. The guard reports that a vehicle is now positioned behind the warehouse and several individuals appear to be loading equipment.

PARTICIPANT QUESTIONS: What can the company realistically achieve in the next 35 minutes? Does it possess any authorised mobile response capability? Can exits be observed safely, can vehicle details be recorded, can CCTV footage be preserved and can access controls be used without increasing danger? Who keeps police updated, and what information would actually help responding officers?

DIRECTING STAFF NOTES: The purpose is to reinforce the difference between detection and intervention. Participants may become frustrated by the police response time. That is the learning point. Determine whether anyone knew the realistic response time before the exercise and whether the existing security design was built around that delay.

SUGGESTED RESPONSE: Personnel should avoid unnecessary confrontation. Available CCTV, vehicle details, descriptions and direction of travel should be preserved and passed to police. Facility controls may be used where safe and appropriate, but measures that could trap offenders and provoke confrontation should not be improvised without prior assessment. Management should maintain a clear communication channel with police while simultaneously determining which critical assets may be affected.

Inject Four – Critical Asset Loss

Police arrive after the offenders have left. Initial examination indicates that approximately USD 70,000 of equipment has been stolen. One missing item, however, is a specialised control component required by a current project. Replacement lead time is estimated at six weeks and the project has only one spare.

PARTICIPANT QUESTIONS: Which is the more significant loss: the USD 70,000 of stolen property or the critical control component? Who informs the affected operation? Can equipment be transferred from another project, who can authorise that transfer, and why was the component stored in the same manner as ordinary inventory? At what point does the burglary become a business-continuity incident?

DIRECTING STAFF NOTES: This inject returns the exercise to operational criticality. The financial value of an asset and its business value are not always the same. Participants should identify when responsibility expands beyond security and what continuity decisions need to occur while the police investigation is still underway.

SUGGESTED RESPONSE: The organisation should immediately assess the operational consequence of the missing component and consider alternative stock, transfer from another project, emergency procurement or temporary operating changes. The criminal investigation and continuity response should proceed in parallel. Management should reassess whether critical components require separate storage, additional controls, redundancy or distribution between locations.

Inject Five – The Contractor Question

During the investigation, access records show that a maintenance contractor entered the warehouse three times during the previous month to service electrical systems. CCTV shows that one member of the maintenance team spent several minutes near the location from which the critical component was later stolen. There is no evidence at this stage that the contractor was involved.

PARTICIPANT QUESTIONS: Who investigates the information and who owns the contractor relationship? Is access immediately suspended, can the company identify the individual personnel who attended and were they escorted? What access did they genuinely require? Who decides whether other company sites using the same contractor should be notified?

DIRECTING STAFF NOTES: The exercise should not encourage unsupported accusation. The objective is to test contractor management, access records, evidence preservation and information sharing between Security, Operations and Procurement. Participants should distinguish reasonable precaution from an assumption of guilt.

SUGGESTED RESPONSE: Relevant records and images should be preserved and provided to the appropriate investigative authority. The company should review access history, supervision and need-to-know restrictions without making unsupported allegations. Access permissions may be adjusted on a risk basis and other potentially exposed facilities should be identified. The event should trigger a wider review of contractor controls rather than a narrow focus on one individual.

Exercise End State and Debrief

Police recover some of the stolen equipment several days later, but the critical component is not recovered. Operations continue because management authorises transfer of the spare component from another project, leaving the company without redundancy until a replacement arrives. The debrief should ask at what point the event became a business-continuity incident rather than simply a burglary and what changes are required to alarm escalation, contractor responsibilities, police notification, guard response, critical-asset classification and continuity planning.

Directing Staff Guidance

The exercises should not be treated as examinations that participants pass or fail. Their purpose is to expose assumptions before a real incident does. Directing Staff should repeatedly challenge phrases such as 'we would notify management', 'we would call security', 'we would contact the police', 'we would evacuate' or 'the guards would respond'. Each answer should be followed by a more precise question: which person, which number, which authority, which route, which location, which capability and what happens if the first option does not work?

The most valuable outcome is a short action register that converts ambiguity into an arrangement. Weaknesses should be grouped around people, communications, authority, external response, physical protection and continuity. Every corrective action should have a named owner and completion date. The exercise is not finished when the discussion ends; it is finished when the vulnerabilities revealed by the discussion have been addressed or formally accepted by management.

Endnotes

[1] International Organization for Standardization, ISO 31000:2018, Risk management — Guidelines. The 2018 edition was reviewed and confirmed in 2023 and remains the published edition while a third edition is under development. https://www.iso.org/standard/65694.html

[2] International Organization for Standardization, ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements. ISO describes the standard as a framework for protecting against, reducing the likelihood of, and ensuring recovery from disruptive incidents. https://www.iso.org/standard/75106.html

[3] UK National Protective Security Authority, Protecting Your Assets. NPSA describes Deter, Detect, Delay, Mitigate and Respond as complementary protective-security principles and states that detection should verify an attack and initiate the response. https://www.npsa.gov.uk/threat-and-risk-management/protecting-your-assets

[4] UK National Protective Security Authority, Protecting Your Assets — Asset and Within Site guidance. NPSA recommends tying protective measures to response requirements and exercising response plans, including consideration of the potential length of response times. https://www.npsa.gov.uk/threat-and-risk-management/protecting-your-assets/asset and https://www.npsa.gov.uk/threat-and-risk-management/protecting-your-assets/within-site

[5] UK National Protective Security Authority, Security Control Rooms Guidance. The guidance stresses clear communication between control-room staff, patrolling officers and response personnel and the need for backup procedures if primary communications fail. https://www.npsa.gov.uk/system/files/documents/73/38/Control%20Rooms%20Guidance%20Dec%202016.pdf

[6] ProtectUK, Managing Risk and Business Continuity. The guidance describes incident management through command, control, coordination and communication and emphasises escalation, stakeholder information and business continuity. https://www.protectuk.police.uk/advice-and-guidance/risk/managing-risk-and-business-continuity

[7] US Cybersecurity and Infrastructure Security Agency, Physical Security Considerations for Temporary Facilities, September 2025. CISA recommends coordinating emergency action plans with local law enforcement and first responders and exercising plans to assess capability and identify gaps. https://www.cisa.gov/sites/default/files/2025-09/Physical_Security_Considerations_for_Temporary_Facilities_20250915_508.pdf

[8] ASIS International, Enterprise Security Risk Management Guideline, 2019. The ESRM approach aligns security resources with organisational strategy and places security professionals in partnership with asset owners to identify and prioritise assets and risks. https://store.asisonline.org/enterprise-security-risk-management-guideline-2019-softcover.html