Crisis management corporate guidelines
Contents
Corporate guidelines 1
Express kidnapping 2
Carjacking 4
Extortion 6
Emergency repatriation 12
Managing the media 16
Specialist response consultants 18
Kidnap procedure for the head office 21
Kidnap procedure for local management 26
Hostage survival 31
Corporate guidelines

This booklet is designed to help organizations deal effectively with a range of crises, ranging from express kidnapping to dealing with the media. Each of the nine sections provides advice on dealing with a particular crisis that may occur.

We look first at express kidnapping, which is becoming increasingly prevalent in many parts of the world. We suggest precautions to take and give sensible advice on what to do if you do fall victim.

Carjacking, which is particularly common in parts of Pakistan, South Africa (Johannesburg), Nigeria, Kenya (Nairobi) and Brazil (São Paulo), is considered next. Some cars will be more attractive to carjackers than others but this does not mean that there is such a thing as a ‘safe’ car. We give advice on precautionary measures, plus what to do in the event of and following a carjacking incident.

The third section examines what to do in the event of an extortion. This can take a number of forms in terms of the target, type of threat and concession that an extortionist demands.

We then provide basic information on planning and implementing an emergency repatriation. Companies with executives living in or travelling to countries where the security situation can deteriorate at short notice are well advised to have repatriation contingency plans in place.

If managed properly, the media can be very helpful; if managed poorly, it can be very damaging. We advise on how to prepare for and manage media interest following a kidnap incident.

The next two sections, kidnap procedure for the head office and kidnap procedure for local management, together help you manage your immediate response to a kidnap incident. The first is designed for a corporation’s head office; the second for local management. This second section titled ‘Kidnap procedure for local management’ is designed to be reproduced on company letterhead and circulated as an instruction document to key personnel. These two sections provide comprehensive advice on crisis management planning, plus what immediate actions should be taken in the event of an incident in preparation for dealing with negotiations, the media, the authorities and the victim’s family.

In the final section, we provide guidelines to raise awareness and give essential advice on how to behave during a hostage incident to minimize the risk to life. Incidents of kidnap, detention, siege or hijack take place with little or no warning and anyone can be in the wrong place at the wrong time. No two incidents will be the same and outcomes are highly unpredictable, but this booklet will provide your organization with tools to deal effectively with a crisis.
Express kidnapping

An express kidnapping can take a number of forms, with a victim forced to:

- go to an ATM machine and withdraw the maximum daily limit (it is common for a victim to be held overnight to withdraw two days’ limit);
- show their account balance on screen, withdraw the maximum daily limit and agree to pay further amounts up to their account balance over a particular time period (there will be the threat of violence for non-payment);
- hand over all the cash, credit cards, PIN number information and valuables on their person or in their vehicle;
- return to their home and hand over all the cash and valuables on the premises.

Precautions

Express kidnappings can happen anywhere in the world. To minimize the chance and consequences of an incident you should:

- only carry a small amount of cash, which can be handed over under duress;
- only carry bank or credit cards if you are actually planning to use them;
- not carry more than one bank or credit card that can be used at an ATM;
- make sure that your ATM card has a low daily withdrawal limit;
- arrange to have cards that do not let you view the account balance on screen. If this is not possible, maintain a low balance in the account.

Awareness

Be aware of the most likely times and locations for express kidnapping. Avoid:

- poor or secluded areas of towns or cities;
- dimly lit streets at night (if you have to walk at night, stick to well lit streets in busy areas);
- driving along quiet roads, especially at night;
- stopping at traffic accidents (they may be staged so keep driving);
- stopping at traffic lights late at night;
- parking in badly lit or deserted areas;
- leaving a restaurant, bar or nightclub late at night;
- hailing a taxi in the street, especially late at night;
- withdrawing cash from an ATM when there are few people on the street;
- starting a conversation with strangers in the street when there are few people around.

If you are the victim of an express kidnap

- Always assume that the criminals are armed.
- Do not resist.
- Remain calm.
- Do not start shouting for help.
- Do not try to escape unless you are absolutely sure you can get away.
- Do not make any sudden movements that might startle the criminals or be interpreted as an attempt to resist or escape.
- Do not hesitate if told to move and do so in a controlled manner.
- Listen carefully to instructions and do as you are told (if instructions are difficult to hear, ask politely but firmly for them to be repeated).
- Do not try to argue or make provocative comments.
- Do not stare or make eye contact with the criminals.
- Look away to indicate that you have no intention of identifying them at a later date.
- Keep your hands in view at all times so there is no danger of the criminals thinking that you are reaching for a weapon.
- Cooperate if told to drive your car.
- Do not pretend that you have lost your keys or try any fancy maneuvers.
- Cooperate without hesitation if told to handover your valuables, credit cards, PIN number, or details of your daily cash limit.
- Cooperate fully when cash is being withdrawn.
- If asked to provide the rest of the money shown in your balance at a future time, agree and ask for instructions.
- Assure the criminals that you will not tell anybody, to give the appearance of cooperating fully.

**When you are released**
- Obey any instructions.
- Move away in a controlled manner; do not panic and run.
- Make your way to a populated place where you will have protection.
- Call your family and reassure them that you have not been harmed.
- Write down all details of the incident and what you have lost, while the incident is still fresh in your mind.
- Cancel any lost credit cards immediately.
- Report the incident to the police, even if they may not take any action.
- Consider involving the police in an entrapment operation if you have agreed to make future payments.
- Report the incident to your national embassy if you are in a foreign country.
Carjacking is a growing crime in many countries but is particularly prevalent in Pakistan, South Africa (Johannesburg), Nigeria, Kenya (Nairobi) and Brazil (São Paulo).

It can happen at any time and an attack may be opportunistic or targeted. Some cars will be more attractive to carjackers than others but that does not mean that there is such thing as a ‘safe’ car.

Most carjackers want to steal the car and any valuables in it, not harm the occupants. They will be armed but will probably only use violence if they meet resistance or are confronted by the police.

The safety of the occupants in the vehicle must be the absolute priority.

If you are living in, or visiting for a long period, any countries where carjacking is prevalent you should:

• take a defensive driving course (this should include driving along regular routes to identify high risk points – such as deprived areas, traffic lights, unlit, remote or slow stretches of road – and safe places – such as hotels, police stations, hospitals and shopping centers. Note any diversions which would enable you to confirm whether your car was being followed – such as gas station forecourts, loop roads and roundabouts);
• get a briefing on incident prevention and how to react during a carjacking.

Prevention
Whenever possible, avoid driving yourself and use a local driver. If this is not possible you should:

• drive a common make of car that is unlikely to be attractive to carjackers and make sure the vehicle is well maintained;
• make sure the car has an alarm and steering lock and is always locked when unoccupied;
• consider utilizing tinted windows (although in some countries this is illegal);
• travel with more than one person in the car or in convoy with another vehicle;
• leave enough space between you and the car in front to give yourself an escape route;
• seek advice on high risk areas and dangerous times (usually after dark) and avoid driving in these areas;
• plan your route before setting out and always know exactly where you are;
• vary your travel routine;
• be alert to the possibility that you might be followed and take evasive action as quickly as possible if you are followed;
• be fully aware of other vehicles in front and behind you – particularly when entering a cul-de-sac – and look out for cars waiting on side roads or off-road parking spaces;
• never offer rides or stop at accidents – drive on to the nearest safe location if you are involved in an accident;
• park in well lit areas, preferably somewhere with a parking attendant;
• check the area for anybody acting suspiciously when you return to your car;
• check that nobody is hiding inside the car, especially in the back;
• install a car phone or carry a mobile to call for help if you have a flat tire, breakdown or accident.

If in doubt, take evasive action and drive to a busy area or a police station for protection.
What to do during a carjacking

During a carjacking incident you may be threatened with a weapon. Do not resist or try to escape. Remain calm and:

• obey all instructions given by the carjackers;
• avoid making sudden movements, but do not hesitate when told to move;
• answer questions truthfully, especially about the car;
• do not ask questions or make provocative remarks;
• avoid making eye contact or showing any signs of recognition;
• keep your hands in view so that there is no danger that the criminals think you are reaching for a weapon;
• express gratitude for any concessions offered;
• tell the carjackers if you are carrying a mobile phone and suggest turning it off to prevent any incoming calls from startling them.

When you are released

• Obey instructions.
• If the carjackers have their own car, do not look at their car to remember details of make, color, number plate etc.
• Call your family and/or office once the carjackers are out of sight to reassure them that you are alright and arrange to be picked-up.

Reporting an incident

Whether you are involved in, or just witness, a carjacking, you should report it as quickly as possible. If you are aware of a carjacking incident you should:

• decide whether or not to inform the police and if you do, make sure you go to a high level in the right department. Stress to the police that the driver is still with the carjackers and that they must not do anything to endanger life;
• decide whether to contact the victim’s family or company executives. If the family is contacted, somebody should be sent to their home to provide support. Give the family a contact number in case the victim calls home;
• place a vehicle on stand by to pick-up the victim on release.

On release

• Send a vehicle to pick-up the victim.
• Inform the family about the incident if they do not already know.
• Contact the police to tell them of the release and provide details of the stolen vehicle.

After the incident

• Debrief the victim to get the full story and learn lessons for the future.
• Talk to the victim to see if they or their family need time off or counselling.
• Report the incident to the relevant embassy if the victim is not a national of the country where the incident has occurred.
• Provide the police with a full report.

Most carjackers want to steal the car and any valuables in it, not harm the occupants.
These guidelines are designed to assist your response to an extortion incident. They are not designed to provide a definitive answer to all the issues that you may need to address.

An extortion can take a number of forms in terms of the target, type of threat and concession that is being demanded by the extortionist(s).

**The targets**
These can include companies, official organizations, including government agencies, families and individuals.

Before deciding on how to respond to a threat, it is important to establish who is the target. If a company assumes responsibility when the actual target is a company employee, it may increase the expectations of the extortionist(s).

**Extortionists**
The characteristics of extortionists will often depend on the part of the world where the incident is taking place.

Terrorist/guerrilla groups make ‘war tax’ or ‘protection money’ demands against companies and individuals in Colombia, the Philippines, Yemen and Assam (north-east India). Mafia gangs operate in many of the states of the former Soviet Union. Organized criminal gangs are common in Latin American countries, China and parts of Africa. Individual criminals are most common in the developed world.

It is important to identify whether an organized group or an individual is carrying out the extortion. This will help determine whether an attempt by law enforcement to arrest the extortionist during a telephone call or when retrieving the ransom, is likely to eliminate the threat.

**The threat**
Extortionists may threaten to carry out one or more of the following: kill, kidnap or cause injury to personnel, plant a bomb, damage property or possessions, introduce a computer virus or release confidential commercial or personal information. In order to formulate your response plan, you will need to assess the extortionist’s ability to carry out the stated threat if the demand is not met.

**Prior planning**

**Threat assessment**
Assess the degree of risk specific to the area and the type of extortion that you might face. By being aware of the type of extortions that may occur and the likely perpetrators, you can take measures to reduce the risk and start putting together an incident response plan.

**Professional assistance**
Establish in advance whether local law enforcement could assist during an incident. It is important that you identify which law enforcement agency and, if possible, which specific people to approach in advance.

It is also useful to seek help from specialist response consultancies both in the planning and training stage and during an incident. They can help you with advance planning and train staff to manage the response. Law enforcement agencies and consultancies can also advise whether other companies/families are facing a similar threat, and details of similar incidents that have taken place previously. This information can assist you during the assessment process.
Management committee

Identify a management committee of three or four senior executives or family members who will be responsible for managing the response to an incident. Ideally, management committee members should be trained and rehearsed so they are aware of their roles and responsibilities in advance of any threat extortion.

Receipt of a threat

Telephone

An extortion by telephone may come in to anyone in the company or an employee at home. It is not possible to prepare everybody in the company to handle such a call. However, the most likely recipients such as switchboard operators, assistants to senior executives, staff in product complaints departments and security personnel should be prepared for such a call. Below is a list of points to follow:

The recipient should

• Write down the message and any useful background information (see checklist on page 9).
• Inform his/her manager, who should alert a senior executive, the security manager or a management committee member.
• Be briefed to keep the call confidential.

Preparing the response

• Get the management committee together to make a detailed assessment of the situation (see checklist on page 9).
• Decide upon a response strategy.
• Appoint a communicator. This person should be given a false name and title.
• Prepare a detailed briefing on the points for any future call from the extortionist.
• Allocate a dedicated telephone line and install a tape recorder.
• Brief the recipient of the original call that, if the extortionist calls back again, they should instruct them to call back on the dedicated number.
• Give the same instruction to anybody else who may receive the next call.

Handling further calls

• The communicator should write down the extortionist’s message and pass on the points that have been decided by the management committee.
• Record all calls. Make a copy of the tape and type a transcript. Store original tapes in a secure place to use during any future legal action.
• The management committee should assess the tape, agree on points for the next call and brief and rehearse the communicator.
Written communications

Addressee
Written communications may be addressed to an individual by name or title. The latter case indicates that the extortionist does not have detailed background information about the company and probably poses less of a threat than one who uses an individual's name.

Methods of delivery
Delivery may be by normal mail, by courier or with an item such as a bunch of flowers or box of chocolates. It may be handed to a third person with access to the target of the threat. If the communication is by mail, a company or individual can buy time by claiming that it hasn’t arrived and asking for another copy to be sent.

Actions on receipt
- Avoid handling the letter and packaging to preserve evidence.
- Keep a record of anyone who has handled the package.
- Make a written record of all the information on the outer packaging and also type up (do not photocopy) a copy of the written communication.
- Place originals in a secure container.
- Brief all those who are aware of the communication to keep all information about it confidential.
- Carry out an assessment of the communication.
- Prepare for follow-up contact by the extortionist by checking all incoming mail before it is sorted centrally.
- Decide whether or not to respond and if you do, what to say.

Verbal messages

Verbal messages are rare and almost exclusively used by extortionists in a rural environment. A verbal message may be given to an employee of the extortion target.

Actions on receipt
- Question the person delivering the extortionist’s message to obtain all relevant information. This should include the exact wording of the message, details of the appearance, dress, weapons carried and transportation of the extortionist(s), the number of people present during delivery of the message, an indication of what group or individual is responsible, the method provided for a response and when a further contact can be expected.
- Brief the person delivering the message to maintain strict confidentiality.
- Assess the content of the message and the circumstances under which it was delivered (see checklist on page 9).
- Decide whether or not to respond and if you do, what to say.

Electronic messages

Extortionists may use the internet or company websites to deliver messages. This might mean that an incident becomes public knowledge very quickly. You will need to try and get the extortionist to change to a more confidential means of communication and temporarily close down your site.
Checklist

**Telephone threats**

Give the following checklist to anybody who may receive a call from an extortionist. Advise them to ask the following questions:

- What is the threat you are making?
- What is the demand?
- Why are you targeting the company/family?
- What organization do you represent?
- When will you make contact again?
- How will you make contact again?

They should also note:

- the time of the call;
- the time the call finished;
- the name of the recipient;
- the date;
- the caller’s voice: male/female; loud/soft; high/deep; aggressive/normal; local/regional/foreign accent;
- speech delivery: educated/fast/normal/slow/deliberate/distorted/lisp/stutter;
- caller’s language: poorly educated/uneducated;
- their manner: calm/irate; rational/irrational; coherent/incoherent;
- background noises: factory/office/residence/animals/children/traffic/music;
- the phone: private/pay phone/mobile.

**Assessment**

Before deciding on how to respond, the management committee should carefully assess the content of the message and method of delivery, according to the following points:

**Method of delivery of the threat**

- How was the threat delivered?
- Could there be doubt that you have received the communication?
- Could you safely justify non-receipt?

**Credibility of the threat**

- Is the threat credible?
- Is there an immediate threat?
- Is the threat likely to be carried out without further contact?
- Can measures be taken to safeguard against the threat?
How much time is there before a response is required?

Likely identity of the extortionist(s)
• Is an individual responsible?
• Is a gang or group responsible?
• If it is a gang or group, are they identifiable?
• Has the likely group carried out similar threats?
• Is an attempted arrest operation a safe option?
• Is this a multi-target extortion?

Time available before a response is required
• How much time is there before a response is required?

Law enforcement assistance
• Can law enforcement agencies provide protection?
• Can an arrest operation be attempted?

Response to the demand
• Can the demand be safely ignored?

If the demand can be ignored, what contingency plans should be made to:
• increase protection of those at risk;
• prepare for further contact from the extortionist(s);
• explain the lack of response to the initial communication.
If the demand cannot be ignored, what actions need to be taken?

Response options
The target of an extortion will have a number of options to respond to the threat including:

- doing nothing is sometimes a credible option in order to discourage the extortionist;
- making excuses for not complying to test the resolve of the extortionist and discourage further contact;
- negotiating for a lower demand or some other concession;
- cooperating with the law enforcement agencies to set up an arrest operation;
- using the local community to put pressure on the group to discontinue;
- moving people at risk away from the area on a temporary or permanent basis;
- conceding to the demands.

If you decide not to respond, you must have contingency plans in place in case the extortionist does contact you again. These plans must include a credible reason for ignoring the original approach. You can: blame a poor postal system resulting in non-receipt of the letter; ask who the original letter was sent to and offer to check; state that the decision maker is away and the matter is pending his/her return; explain that you have received many similar approaches, so it is difficult to identify a serious demand.

Conclusion
You can discourage the majority of threat extortionists from continuing by not responding to the initial communication or by introducing difficulties during communication.

By testing the resolve of the extortionist(s) it is easier to assess the seriousness of the extortion and decide on a response plan.
The security situation in many countries can deteriorate with little warning, putting company executives and their families who are living or visiting there at risk.

Companies with operations in high risk areas should have repatriation contingency plans in place and be ready to implement them when necessary. These guidelines are general and not comprehensive. Some points may not be relevant in every country. Detailed country specific plans should be produced for each country if possible.

**Emergency management team**
Form a small emergency management team to monitor developments and make and implement decisions. They will also act as the focal point for employees in the country of risk and senior executives at the regional or head office.

**The warden system**
Establish a warden system to allow rapid exchange of information and to help control an emergency repatriation. Divide families into groups of 10-15 people by residential area and appoint a warden to each group. Give everybody in each group the warden’s name and contact details, and those of a deputy. The warden should report to, and be under the control of the emergency management team.

**Proactive information gathering**
Up-to-date information is vital for making decisions proactively and not retrospectively, when it may be too late. Information on developments can be obtained from:
- international radio and television;
- the internet for US State Department advisory reports see www.travel.state.gov and for UK Foreign Office country reports see: www.fco.gov.uk/travel;
- local embassies;
- other foreign companies operating in the country;
- local governmental, military and business sources;
- commercial information sources.

**Repatriation of personnel**
As the security situation deteriorates, initiate phase one of a ‘two phase’ repatriation to reduce the number of personnel in country. You need to establish ‘trigger’ points to assist the decision making process. Whenever the situation and communications permit, the decision to repatriate personnel should be taken jointly between head/regional and country management.

**Phase one**
First trigger: the situation has deteriorated, and indications are it will continue, putting personnel at risk.
- Non-essential personnel, including visitors, should leave, preferably on scheduled flights.
- Stop other company visitors, both business and private, from entering the country.
- Centralize remaining personnel at a safe location.
Phase two
Second trigger: the situation has deteriorated to an extent that there is a real risk to the safety of personnel.

• All remaining personnel should leave by the safest available route.
You will need to decide early on how to respond to requests by locally employed personnel and their families to be evacuated from the country.

Preparations for leaving
• Check the capacity of company vehicles to make sure that remaining personnel can be transported.
• Start liaising with country managers of international airlines operating scheduled flights. Country managers will be able to advise on whether flights to the country are being suspended.
• Buy ‘open’ airline tickets for remaining personnel.
• Identify other possible exit routes: road, rail, sea or river, private aircraft, another airport, on foot.

Communications
Communication lines may be down or overloaded, so you need to identify stand-alone communication systems as a back up. These include:

• international satellite mobiles;
• satellite phones;
• radios (embassies, major airlines and oil companies often have radio networks).
You should have lists continually updated and readily available with contact details of in-country personnel, embassies and other foreign companies. Country management should have 24-hour contact numbers of relevant regional/head office personnel.

Contingency planning
Ensure that staff residences have:
• a seven-day store of food and drinking water;
• a standby electricity generator;
• an emergency reserve of water for washing and toilets;
• flashlights with spare batteries;
• candles and matches;
• a gas, propane or generator operated refrigerator in hot countries;
• a medical pack;
• a gas operated cooker;
• fire extinguishers;
• battery operated radio and television;
• an alternative company internal communication system.
It is often also useful to have a bicycle at the residence to travel around the local area.
Identify early on how you will securely store or evacuate valuable personal property.

Personal possessions
Space is likely to be limited for evacuees’ personal luggage. Instruct personnel to pack one small bag with essential items including one set of warm clothing. Make arrangements early on to evacuate pets or identify people who will care for them in the absence of the owner. Identify early on how you will securely store valuable personal property.

Vehicles
Have a reliable cross-country vehicle in a secure location adjacent to each residence. The vehicle should have:
- a full fuel tank;
- spare fuel;
- containers of drinking water;
- tools including a jack, jumper cables and tow chain;
- country maps;
- essential spare parts, such as a fan belt, fuses, light bulbs and batteries;
- high calorie food;
- vehicle radios or mobile phones;
- satellite navigation equipment;
- flashlights;
- a first aid kit;
- a fire extinguisher;
- for desert climates a shovel, sand channels, tarp and a compass;
- for cold climates snow chains, survival blankets and equipment to boil water.

Local assistance
Identify local personnel who would be willing to accompany evacuating groups to act as guides/interpreters.

Other organizations’ evacuation plans
You can take advantage of other organizations’ evacuation plans.

Other companies
- Identify if other foreign companies have plans and are willing for you to be part of their plan (e.g. offshore oil-rig supply companies, sea/air freight companies).
- Agree on procedures for ongoing liaison and for activating the plan.

Diplomatic missions
- Make sure all expatriate employees plus all visitors register with their national embassy.
- Find out if the embassy has emergency evacuation plans and whether the company can participate if necessary.
- Find out what nationalities will be allowed to take advantage of which country’s evacuation plans.
- Get contact details of the diplomat responsible for coordinating the plan.
Documentation

- Check that all passports are valid and will not expire in less than three months.
- Have duplicate copies of all identification.
- Check that everyone has the necessary visas and clearance certificates for exiting the country.
- Make sure that all those who are to be repatriated carry proof of their nationality.
- Make sure that each group has at least US$2,500 in cash, or the equivalent in another hard currency, a reasonable amount of local currency and any accepted credit cards.

Security points

- The management team should issue regular security advice notices to all personnel. These should cover matters such as curfews, out-of-bounds areas, locations of ongoing or planned demonstrations, situation assessments and important phone numbers.
- All personnel should maintain a low profile and not become involved in political discussions or arguments.
- Personnel should not wear military style clothing or anything that advertises their nationality or the company for whom they work. Remove logos and national flags from vehicles and buildings.
- Remove name boards that identify premises or residences as belonging to foreign interests.
- Advise all personnel to avoid demonstrations or marches and move people living in the neighborhood or along the route to a safe location.
- Move any personnel who live near potential targets (foreign embassies or company premises, military bases, government buildings), gathering places for political meetings or demonstrations (buildings belonging to foreign governments or companies, universities, mosques) to a safer area.
- Set up a permanently manned phone number for people to report incidents or get advice.
- Centralize personnel in groups or at a single safe location (corporate or safe diplomatic premises, international hotels).
- Liaise with local law enforcement and/or security companies to establish what protection will be provided.

Post repatriation considerations

- Appoint a local executive to manage your business interests.
- Appoint local executives to look after the security of business premises and residences that have been left empty.
- Make sure that local management has the necessary legal documentation to continue to run the business.
- Make sure that local management has access to funds to pay local staff and settle bills.
- Establish communications to local management.
- Monitor the situation in the country to assess when an expatriate presence can be re-established.
- Identify routes back to the country.
Managing the media

News of a kidnap can become public knowledge fast. The media will try speaking to any witnesses of the abduction, family members or colleagues of the victim, and law enforcement agencies. Journalists have a job to do and will pursue a story.

You need to encourage their cooperation and avoid antagonizing them by being dismissive. If managed properly, the media can be extremely helpful. If managed poorly they can be very damaging.

If you can find friends, family members or employees who have contacts within media organizations, you may be able to use them to suppress coverage of an incident. However, you still need to have a contingency plan in place for handling the media. Update it regularly as an incident develops.

Preparation

- Nominate which individuals will form the crisis management team in the event of an incident.
- Select and train somebody to act as a spokesperson. Have a second person as backup in case the spokesperson is not available at the time of the incident.
- Companies with operations outside their home country should have a trained spokesperson at head office and in each country.
- Make sure there is a dedicated phone line for handling media calls during an incident. It should have recording equipment attached.
- Make sure you have the equipment available to monitor radio, television, newspaper and internet reports.
- Put together a contact list of senior people within the local press, radio and TV stations.

During an incident

If members of the public have witnessed the incident, you won’t have much time before the media makes contact. You will need to action a media management plan straight away.

- Brief your spokesperson about the incident.
- Give the spokesperson’s name and contact details to the rest of the company and the victim’s family. Brief them not to speak to the media but to refer any inquiries to this spokesperson.
- Have a defensive media statement ready to use.
- Identify questions that the media might ask and prepare a questions and answers document.
- Review and update your defensive media statement, and questions and answers documents regularly as the incident develops.
- Ensure that any statements and questions and answers documents are sent to the nominated spokesperson in other relevant countries. It is important that the same message is given out throughout the organization.
- Monitor newspapers, magazines, radio, television and internet sites for any coverage of the incident. The crisis management team will have to decide whether to correct any inaccurate or speculative reporting, or to ignore it.
- Make sure there is ongoing communication between the spokesperson and the crisis management team. Spokespersons abroad must keep the main spokesperson briefed on any developments where they are.
- The spokesperson must work closely with the crisis management team and mutually agree on any statements or questions and answers documents.

Defensive media statements

- Information given to journalists must be factually correct. Avoid disclosing anything sensitive that could endanger the life of the hostage, be detrimental to the morale of their family or company members, or could hinder negotiations with the kidnappers.
Before giving any information to a journalist you must

- Establish their credentials.
- Ask what information they already have.
- Clarify the sources of that information.

If the journalist has background knowledge you should

- Admit that there has been a kidnap.
- Relate publicly known facts concerning the abduction.
- State that it would be dangerous to make any further comment as someone’s life is in danger.
- Seek understanding and sympathy.
- Request responsible reporting. Stress that this is in the best interest of the victim and their family during a highly emotional and stressful time.
- Refuse to speculate.

No details should be provided about

- The kidnappers’ demands.
- Your negotiating strategy.
- Contact with law enforcement agencies.
- The victim, other than to confirm his/her identity.
- Any information about the victim’s family.
- The assets of the company or the victim’s family. This must be played down.

If the journalist is investigating a rumor

- Express surprise at the call.
- State that you are not aware of the rumor and ask what information they have.
- Thank them for the call and say that you will look into it.
- Ask for contact details so you can call back once you have investigated the situation.

Note: If there is a large volume of calls, the crisis management team must decide whether to continue to handle them individually or issue a verbal or written statement.

Using the media to advantage

During a kidnap there are times when you can use the media to send a message to the kidnappers, or to let the hostage know that he/she has not been forgotten. This may be necessary during a lengthy kidnap in order to break a period of silence, or pressure the kidnappers to prove that the victim is alive and well.

To achieve this you can:

- broadcast veiled messages and music over radio stations (hostage ‘morale boosters’).
- ask a friendly journalist or broadcaster to issue a general news item on the kidnapping that does not directly implicate the victim’s family or your company.
- arrange an emotional interview with a close family member of the victim.
- broadcast or publish an article about the emotional stress the family is suffering, without involving them directly.
During a kidnap, the deployed response consultant is an advisor only, not a decision maker. He or she will assess any developments, identify the options and recommend a course of action. It is always the responsibility of the appointed/nominated crisis management team to make decisions.

Reporting an incident

In the event of an incident call the 24-hour emergency number immediately. You will receive advice over the telephone and a consultant will be deployed to the location of the incident. A second consultant may be sent to the head or regional office, as necessary.

Whoever makes the initial phone call should provide as much of the following information as possible:

- name, age, sex and relationship/executive position of the victim;
- date and time of the kidnap;
- location of the kidnap;
- description of the abduction;
- information about any injuries suffered by the victim;
- law enforcement knowledge and/or involvement;
- media knowledge and any publicity;
- details of witnesses to the abduction;
- the possible identity of the kidnappers and any contact to date;
- name and phone number for future contact.

The response consultancy operations center should

- Assess the information provided.
- Give the caller immediate advice.
- Deploy a consultant to the location of the incident.
- Give the client the name and arrival details of the deploying consultant.
- Provide contact name and telephone number of the case manager.
- Contact the client again with additional advice.

On arrival, the deployed consultant should

- Agree on a time and place for meeting with the client.
- Get updated information and make an assessment, with options and recommendations.
- Advise on policy issues.
- Advise on the crisis management team structure.
- Advise on the selection of a communicator.
- Assist in preparing the communicator’s phone.
- Prepare points for the communicator. Brief him/her and rehearse the points.
- Advise on legal requirements.
- Help prepare defensive media statements and a questions and answers document.
- Advise on reliable contacts within local government and/or law enforcement agencies.
- Brief on information from previous incidents in the country.
- Brief the family on how the incident is likely to develop.
- Be available to the client 24-hours per day throughout the incident.
- Liaise on a regular basis with the case manager at the head office.
Ongoing assistance by the deployed consultant
During long cases, there will normally be two consultants working on a three-week rotation until the conclusion of the incident.

The consultants will
• Assess all developments.
• Identify options for responding to communications from the kidnappers and make recommendations.
• Assist in liaising with third-parties including law enforcement.
• Identify other initiatives that might assist in resolving the problem.
• Brief and rehearse the communicator before each contact.
• Advise on the method, frequency and content of briefings for the hostage’s family.
• Advise on the collection, storage and delivery of ransom monies.
• Advise on the recovery and rehabilitation of the released hostage.
• Remain available to the client until the hostage has been released and debriefed.

Response consultants DO NOT
• Act as the communicator.
• Attend face to face meetings with the kidnappers.
• Provide the money for the ransom.
• Deliver the ransom to the kidnappers.
• Discuss information about the incident without the permission of the client.
• Investigate the crime.
• Attempt to locate or rescue the victim.
• Compete with the local government or law enforcement agencies.

Selecting a response consultancy
There are a number of consultancies and individuals who provide response advice during an incident. This section outlines points for consideration when selecting a response consultancy.

• Experience: the number of cases they have assisted on, the outcomes and the countries in which these have taken place. Does the response consultancy have worldwide experience or is it orientated towards one region or continent? Experience of consultants in a commercial rather than government service capacity is important, as a number of issues will differ.
• Database: information that is stored about previous cases that the response consultancy has worked on and from other reliable sources.
• Country contacts: the knowledge of and contacts within law enforcement and government agencies.
• Legal requirements: knowledge of kidnap related laws, and the documentation required for a deployed consultant to work in a particular country.
• Country offices: local offices to provide updated situation reports, advise on legal requirements and support for clients and deployed consultants.
Individual consultants should go through an in-depth selection process followed by both theoretical and practical case training before being deployed.

- **Linguistic ability**: response consultancies that operate worldwide should have consultants who speak a range of languages.
- **Employment of consultants**: some response consultancies only use consultants who are salaried employees of the consultancy. Others use a pool of retained consultants who are not based at the head office. It is preferable to have consultants who are salaried and work out of the response consultancy’s head office. This ensures better training, ongoing updates on kidnapping in countries, knowledge of current incidents, access to the database, exchange of ideas among consultants, quality control by management and control of the confidentiality of information.
- **Selection and training**: individual consultants should go through an in-depth selection process followed by both theoretical and practical case training before being deployed.
- **Emergency response line**: some response consultancies rely on an automated answering system for incident notification. Others sub-contract to a third-party. In-house, experienced consultants who are available 24 hours a day provide the best response service. Not only will the response be faster, but they can also give immediate advice on what to do.
- **Reserve consultants**: the number of permanent consultants employed will dictate how many cases can be serviced at one time. Ideally, there will be a reserve pool of experienced response consultants within the organization who can be drawn on when necessary.
- **Consultant/head office communications**: communication should be via a secure system, preferably email.
- **Case management**: an experienced senior executive with case experience should monitor all ongoing cases and provide support and advice to the deployed consultants. For long running cases, there should be periodic management visits to the client.

**Questions to ask should include**

- How long has the consultancy been established?
- What are the individual consultants’ backgrounds?
- Are consultants salaried or retained?
- How many commercial incidents has the consultancy and its consultants handled?
- What support does the deployed consultant receive from head office?
- What language capability do consultants have?
- Has the consultancy been involved in litigation following an incident?
- What is the policy for liaising with government and law enforcement agencies?
These guidelines have been produced to complement the following section, ‘Kidnap procedures for local management’. Together they can help you manage your immediate response to an incident.

Although every kidnap will be different, there are common elements to any incident for which you can prepare. It is best practice to have contingency plans in place and key executives trained in advance to manage the response.

**Distribution of kidnap procedure guidelines**

The following section, ‘Kidnap procedures for local management’, is designed to be sent to selected executives who should know what to do in the event of an incident. The guidelines are designed to be typed out on company letterhead and circulated in the same way as other priority instructions to senior executives.

**Contingency planning**

If you have subsidiaries where there is a credible threat of kidnap, extortion or other major security related problems:

- circulate copies of the ‘kidnap procedures for local management’ on company letterhead to selected executives;
- send copies of ‘kidnap procedures for the head office’ on company letterhead to the head office executives who will be informed immediately in the event of an incident.

**To be properly prepared for an incident you should establish in advance**

- Which senior executives should be immediately informed about an incident.
- The legal requirements for informing the authorities. Find out to whom you should report and what the correct procedures are.
- Procedures for managing the media.
- Procedures for informing the family of a hostage and liaising with them either in or outside the country where the incident has occurred.
- Who will act as a communicator.
- Dedicated communication channels to be used throughout the incident between head office and local country management teams.

**Post abduction/extortion demand – immediate actions**

- As soon as you hear about an abduction or extortion demand, contact your specialist response consultants. It is important to inform them as soon as possible about an incident, so that they can give advice during the vital early stages.
- Provide the response consultants with all the information available. They have extensive experience in responding to kidnap and extortion demands, and will be able to help you plan your immediate response.
As soon as the response consultants have been informed about the kidnap, they will be available to give you advice by phone, fax or email.

Flights and visas permitting, a consultant will be with you and/or at the incident location within 24-hours.

- An executive in the country where the incident took place should contact one of the following three nominated head office executives:
  1. Name
     Office
     Home
     Mobile
  2. Name
     Office
     Home
     Mobile
  3. Name
     Office
     Home
     Mobile

- Make sure that these contact details are passed to local offices so they know whom to contact.
- The head office executive who is contacted should write down:
  - the identity of the hostage;
  - the date and time of the abduction;
  - the location and method of abduction;
  - whether there were any casualties at the scene of the abduction;
  - whether the hostage was injured;
  - any demands which have been made;
  - the method used by kidnappers to communicate their demands;
  - the location and contact details of the hostage’s family;
  - whether the family knows about the abduction;
  - actions taken to date;
  - whether local law enforcement is involved or knows about the incident;
  - whether members of the public witnessed the abduction;
  - whether the media knows about the incident and there has been any coverage.

- Establish whether or not the specialist response consultants have been contacted. If not, contact them immediately and pass on all relevant information.

**Note:** as soon as the response consultants have been informed about the kidnap, they will be available to give you advice by phone, fax or email. They will advise on how to stabilize the situation until a response consultant arrives. Flights and visas permitting, a consultant will be with you and/or at the incident location within 24-hours.
Immediate actions
The head office executive alerted to an incident should:
• write down all the available information (see above);
• agree on dedicated contact numbers with the local office and exchange telephone numbers for contact until further notice;
• inform the crisis management team chairman about the incident and call a meeting.

Initial meeting
To open the meeting you should summarize:
• what is known about the incident;
• what actions have been taken to date, both locally and by the head office executive who received first notification of the incident;
• what actions have been taken by third parties, such as the authorities or the media;
• what contact there has been from the kidnappers.

Organization
• Agree on the composition of the crisis management team to manage the response to the incident.
• Decide whether or not to send a head office executive to the country of the incident.
• Decide whether you want a specialist response consultant to deploy to the country of the incident and/or the head office (if this has not already been initiated).

Primary company objective
• Confirm that the primary objective is the timely and safe return of the hostage(s).

Decision making authority
• Agree on and direct decision-making authority between the head office and the local office where the incident has taken place.

Company policy
• Agree on whether the company will manage the response or delegate responsibility to a third party.
• Agree that the company will enter into dialogue with the kidnappers for the release of the hostage(s).

The hostage
• Take out the hostage’s personal file.
If the hostage is not a national of the country where the incident has occurred, their national embassy should be informed.

Confirm 24-hour contact details for all personnel who will be involved in managing the incident.

The family
Decide whether the head office or the local office will take responsibility for informing the hostage's family of the incident, and for ongoing liaison. This will depend on where the family lives.

- Get next of kin contact details and inform them of the incident right away.
- Appoint somebody to act as the dedicated point of contact throughout the incident and provide the family with contact details.
- Agree on procedures for helping and protecting the next of kin.
- Any letters sent to the family from the hostage or kidnappers should be opened and read by somebody from the crisis management team.

The media (see ‘Managing the media’ guidelines on page 16)

- Appoint a company spokesperson.
- Prepare a defensive media statement but only use it if the media approaches you.
- Prepare a questions and answers document.
- Coordinate the handling of the media with the local office and send defensive media statements and questions and answers documents to them.
- Start monitoring the media for coverage of the incident.

Legal

- Get information about the local laws governing kidnap in the hostage's home country and the country of the incident.

Government liaison

- If the hostage is not a national of the country where the incident has occurred, their national embassy should be informed. Check with the local office to see if this has already been done.

Administration

- Assign responsibility for maintaining a record of events, and collecting and securely storing all documents relevant to the incident.
- Allocate responsibility for implementing decisions to each member of the management team.
- Confirm 24-hour contact details for all personnel who will be involved in managing the incident.
- Confirm dedicated communications channels for incident traffic.
- Contact the local office crisis management team again and update them on the actions taken and proposed at head office.
- Brief those who know about the incident to keep all information strictly confidential.
- Agree on the timing and venue for the next meeting.
Preparation for initial contact with the kidnappers
The initial contact will most likely be in the country of the incident. It may be in the form of a letter, telephone call or verbal message through an intermediary. This may come within hours or after a delay of weeks. The head office crisis management team should make sure that the local office is prepared for the contact.

Administration
The head office crisis management team should make sure that the local office:

• Has installed a tape recorder on the dedicated telephone line.
• Has appointed and briefed a communicator. This person must be a fluent local language speaker.
• Has prepared a script of points for the communicator to use.
• Knows to send transcripts and translations of any telephone conversations to the head office crisis management team as soon as possible after contact.
• Knows that translations and copies of any written communications should be sent to the head office crisis management team as soon as possible.

The first response from the local office should

• Express concern for the hostage's well being.
• Give information about any regular medication the hostage takes.
• State that the company holds the kidnappers responsible for the safety of the hostage.
• Include a proof of life question for the hostage to answer.
• State that the company is taking the matter very seriously and is willing to enter into a dialogue to find a mutually acceptable solution.
• Agree on a code word for the group to use to identify themselves and eliminate hoax callers.
• Make arrangements for future communications, including means, timings and the communicator's telephone number.

Initial response should NOT include

• Any commitment to or comment on financial demands.
• Any indication that the communicator has the authority to make decisions.
• Any specific negatives, the communicator should be conciliatory but not promise anything or give any indication that the authorities are involved. If the kidnappers suggest this, it should be denied.
• Any financial discussion before proof of life has been received.

Summary
These guidelines provide the head office crisis management team with a checklist of issues that need addressing in the immediate aftermath of an incident. This should provide a strong base from which to manage the response to the incident. As the incident develops, there will be a number of new and complex issues that will need to be addressed. Specialist response consultants will be available to help the crisis management team address these issues.
Kidnap procedure for local management

These guidelines have been produced to complement the previous section ‘Kidnap procedure for the head office’. Together they can help you manage your immediate response to an incident.

A specialist response consultant should be available to a maximum of three people who are nominated to form the decision making team in the event of an incident. The guidelines should be kept strictly confidential.

Although every kidnap will be different, there are common elements to any incident, which you can prepare for. It is best practice to have contingency plans in place and key executives trained in advance to manage the response.

Contingency planning
To be properly prepared for an incident you should establish in advance:

- whether it is a legal requirement to inform the local authorities about an incident.

Find out whom you should report to and what the correct procedures are;

- which communication lines you will use during an incident. You will need a dedicated fax and phone line to the head office and a dedicated landline or mobile phone for use by the communicator;

- procedures for informing the family of a hostage and liaising with them either in or outside the country;

- procedures for handling the media;

- who will act as the communicator.

Immediate actions
As soon as you are aware of an incident, gather the following information:

- the identity of the hostage;

- the date and time of the abduction;

- location and method of abduction;

- whether there were any casualties at the scene of the abduction;

- whether the hostage was injured;

- any demands which have been made;

- the method used by kidnappers to communicate their demands;

- contact details for the hostage’s family;

- whether they know about the abduction;

- actions taken to date;

- whether local law enforcement is involved or knows about the incident;

- whether members of the public witnessed the abduction;

- whether the media knows about the incident and if there has been any publicity;

- description of the kidnappers and the group’s identity;

- immediate contact details for the informant for the next few hours.
Contact your specialist response consultants immediately – either directly or through your head office, depending on your internal procedures. If you contact the response consultants directly, you should let your head office know about the incident.

The specialist response consultants have extensive experience in dealing with kidnap incidents and will be able to help you plan your immediate response. Pass on the information you have gathered (see page 26) and provide whatever assistance and additional information is requested.

As soon as the response consultants have been informed about the kidnap, they will be available to give you advice by phone, fax or email. They will advise you on how to stabilize the situation until a response consultant arrives. Flights and visas permitting, a consultant will be with you within 24-hours.

Agree on dedicated contact numbers to be used for incident response and let the head office know what they are.

Inform other local senior executives about the incident and call a meeting.

**Initial meeting**

To open the meeting you should summarize:

- what is known about the incident;
- what actions have been taken to date, both locally and by the head office crisis management team;
- what actions have been taken by third parties, such as the authorities or the media;
- what contact there has been from the kidnappers.

**Organization**

- Agree on the composition of a local management team to manage the response to the incident.
- Decide whether you want a response consultant to be deployed.
- Decide whether you want an executive from your head office to join the local management team.

**Primary company objective**

- Confirm that the primary objective is the timely and safe return of the hostage(s).

**Decision making authority**

- Establish with the head office crisis management team which decisions must be referred to them and which can be made at local management level.

**Company policy**

Agree with the head office crisis management team:

- whether the company will manage the response or delegate responsibility to a third party;
- that the company will enter into dialogue with the kidnappers for the release of the hostage(s).
If the hostage is not a national of the country where the incident has occurred, inform their national embassy.

Nominate somebody to act as the family’s dedicated point of contact throughout the incident.

The hostage
Take out the hostage’s personal file to establish:
• the contact details of next of kin and family information;
• any listed proof of life questions that can be used in the initial contact with the kidnappers;
• details of any regular medication that the victim takes, so that this can be passed to the kidnappers at the first opportunity.

The family
If the family is resident in the country of the incident:
• get next of kin contact details and inform them of the incident right away;
• nominate somebody to act as the family’s dedicated point of contact throughout the incident;
• agree on procedures for helping and protecting the next of kin.

Any letters sent to the family from the hostage or kidnappers should be opened and read by a member of the local crisis management team first.
If the family’s family lives outside the country of the incident:
• get next of kin contact details and pass them to the head office crisis management team;
• liaise with the head office crisis management team to decide who will inform the next of kin about the incident and who will be responsible for ongoing communication.

The media
Coordinate a media management plan in conjunction with the head office crisis management team (see ‘Managing the media’ guidelines on page 17).
• Appoint a spokesperson.
• Prepare a defensive media statement, but only use it if you are approached by the media.
• Prepare a questions and answers document.
• Start monitoring the media for coverage of the incident.
• Let the head office crisis management team know about any local coverage.

Legal
• Confirm information about the local laws governing kidnap incidents.
• Prepare any written report that you have to submit to the local authorities.

Embassy liaison
• If the hostage is not a national of the country where the incident has occurred, inform their national embassy.
**Administration**

- Assign responsibility for maintaining a record of events, and collecting and securely storing all documents relevant to the incident.
- Allocate responsibility for implementing decisions to each member of the management team.
- Confirm 24-hour contact details for all personnel who will be involved in managing the incident.
- Confirm dedicated communications channels for incident traffic.
- Contact the head office crisis management team again to update them on developments and find out what actions and decisions they have taken.
- Brief those who know about the incident to keep all information strictly confidential.
- Agree on a time and venue for the next meeting.

**Preparation for initial contact with the kidnappers**

The first contact may be in the form of a letter, phone call or verbal message through an intermediary. This may come within hours or after a delay of weeks. If the kidnappers’ first contact is by phone they may call the office, a senior executive, or a member or friend of the family. You should be prepared for all these situations.

**Briefing possible recipients**

- Identify which people might receive the first call and brief them. They should tell the caller to call the dedicated incident number.

**Administration**

- Install a tape recorder on the dedicated telephone line.
- Appoint and brief a communicator. This person must be fluent in the local language.
- Prepare a script of points for the communicator to use.
- Send transcripts and translations of any telephone conversations to the head office crisis management team as soon as possible after contact.
- Translations and copies of any written communications should be sent to the head office crisis management team as soon as possible.

**In your first response you should**

- Express concern for the hostage’s well being.
- Give information about any regular medication the hostage takes.
- State that the company holds the kidnappers responsible for the safety of the hostage.
- Include a proof of life question for the hostage to answer.
- State that the company is taking the matter very seriously and is willing to enter into a dialogue to find a mutually acceptable solution.
- Agree on a code word for the group to use to identify themselves and eliminate hoax callers.
- Make arrangements for future communications, including means, timings and the communicator’s telephone number.
As the incident develops, you will need to address a number of new and complex issues. A response consultant will be available to offer advice and assistance.

Initial response should NOT include
• Any commitment to or comment on financial demands.
• Any indication that the communicator has the authority to make decisions.
• Any specific negatives. Be conciliatory but do not promise anything.
• Any indication that the authorities are involved. If the kidnappers suggest this, deny it.
• Any financial discussion before you have proof of life.
• An offer before a demand has been made.

Written communications
• If you are instructed to collect packages, do so quickly.
• Send at least two reliable people.
• Make a working copy of the message and store the original in a safe place.
• Translate the message.
• Fax or email copies of the original message and the translation to the head office crisis management team as quickly as possible.

Summary
These guidelines provide local management with a checklist to follow immediately after an incident. This should provide a strong base from which to manage the response to an incident.

As the incident develops, you will need to address a number of new and complex issues. A response consultant will be available to offer advice and assistance.
There has been an increase in criminal and terrorist activity throughout the world. Media coverage of incidents has also increased and detailed reenactments in print and on television are common.

Publicity encourages copycats and increases the risk to everybody. Anyone can be in the wrong place at the wrong time, and fall victim to a hostage incident.

The best protection is to be well informed about which countries and areas are high risk. Take sensible security precautions and always be aware of what is happening around you. If the worst happens, know how to behave to maximize your chances of survival.

These guidelines are designed to raise awareness and aid survival during a kidnap, hijack, siege or illegal detention. No two incidents are the same, so it is impossible to give specific advice on every situation.

Kidnap

Kidnappers can be terrorists, guerrillas, criminals or psychopathic individuals. The conditions, treatment and length of captivity can vary enormously from group to group. As a general rule, hostages of terrorist or guerrilla groups are well treated but could be held in captivity for months. Criminal gangs do not tend to treat their hostages well, but the length of the ordeal is often much shorter. The most dangerous kidnapper is the loner who has to act as both jailer and negotiator.

Briefing people in high risk areas

A proper brief can reduce the chance of becoming a victim, and reduce the shock and fear factor in the event of an incident. It should include:

• information about kidnappers’ selection and surveillance methods;
• kidnappers’ actions during an abduction;
• likely treatment during captivity. A briefing by a released hostage can be useful;
• how to behave during captivity;
• what contact details to give to the kidnappers;
• response contingency plans for the family and company.

Hostage behavior. Do

• Think positively.
• Maintain your dignity – be cooperative but not subservient.
• Be yourself.
• Tell the kidnappers about any medication you are taking.
• Try to establish a rapport.
• Request your basic needs.
• Express your thanks for concessions.
• Plan how to protect yourself in the event of a rescue.
• Be aware that you may be made to write dictated letters or read a prepared script. Try to indicate covertly if a statement is dictated.
• Remember any noises to help establish where you were held after your release.
• Establish a daily routine.
• Keep track of time – keep a diary if possible.
• Eat what is provided – divide it into three portions if you are only given food once a day.
Do physical exercises even if there is limited space.

- Take care of your personal hygiene.
- Exercise your mind.
- Do physical exercises even if there is limited space.
- Establish a normal sleep pattern.

**Hostage behavior: Don’ts**

- Resist during the abduction.
- Try to escape unless there is a strong chance of success.
- Antagonize your captors.
- Think you have been abandoned.
- Blame yourself for what has happened.
- Get into controversial discussions with the kidnappers.
- Self negotiate.
- Provide information that could be used to pressure your family or employer.
- Build up an image of your professional importance.
- Speculate what your company or family can or will pay.
- Comment on negotiations.
- Believe everything you are told.
- Be uncooperative – be firm but not confrontational.
- Show recognition of your abductors.

**Assistance by outside parties**

In some cases, you can assist a hostage by:

- asking proof of life questions;
- sending morale booster messages through the media;
- using intermediaries (individuals or humanitarian organizations) to deliver letters and comfort packages.

---

Our consultants have extensive experience in responding to kidnap and extortion demands and will be able to assist you in planning your immediate response.
**Hijack**

September 11th demonstrated a terrifying change in strategy with suicide attacks against ground targets as opposed to hostage taking as a bargaining tool. The crew and passengers in future hijacks will need to assess the identity and purpose of the hijackers before deciding whether to act passively or to try to overpower the hijackers. These guidelines are for hostage-taking hijacks only.

**Before you fly**
- Choose a low profile airline.
- Check the airline’s security procedures.
- Choose a flight that starts from your point of departure, rather than one that is stopping off from somewhere else.
- Book a non-stop flight to your destination whenever possible.
- Avoid a flight share where another carrier is used.
- Travel economy class.
- Dress casually and inconspicuously.
- Avoid openly advertising your nationality, company or status.
- Select a window seat in the middle of the aircraft.
- Do not draw attention to yourself at check-in, in the departure lounge or on the aircraft.
- Do not be drawn into conversation with strangers.
- Be alert to the behavior of your fellow passengers.

**During a hostage taking hijack**
- Remain calm.
- Reassure neighboring passengers.
- Make yourself as unobtrusive as possible.
- Avoid eye contact with the hijackers.
- Listen carefully for instructions from the crew or hijackers.
- Obey any instructions.
- Avoid making any movements that may startle the hijackers.
- Identify the nearest safety exit and an alternative – memorize your route to them.
- Develop a protective action plan in the event that shooting breaks out.
- If a rescue operation takes place do not stand up or look around you to see what is happening. Lie on the floor and listen for any orders from the rescuers.
- Be ready to leave the aircraft as quickly as possible – do not try to recover your personal belongings first.
Siege

Sieges can take a number of forms, from a well-planned operation by a terrorist group, to a failed bank robbery. In any siege incident, inappropriate behavior by a hostage may place not only his or her life in danger but also the lives of fellow hostages.

Hostage behavior. Do's

- Stay calm.
- Try to reassure other hostages near to you.
- Avoid eye contact with the hostage takers.
- Listen to instructions and be cooperative.
- Try to discourage any hostage who is obviously antagonizing the hostage takers.
- Identify exits and your routes to them.
- Plan how to protect yourself in the event of a rescue operation.

During a long siege

- Request basic needs especially if you need regular medication.
- Establish a daily routine for exercise, food and sleep.
- Maintain personal hygiene.
- Lie on the ground during a rescue operation.
- Listen to orders given by the rescuers and obey them quickly.
- Calm down and help anybody else who is panicking.
- When out of the building or vehicle, get well clear.

Hostage behavior. Don'ts

- Antagonize the hostage takers.
- Do anything to draw attention to yourself.
- Make sudden movements that may startle the hostage takers.
- Set yourself up as a hostage leader unless no one else appears capable.
- Enter into conversations about controversial topics.
- Stand up or look about during a rescue.
- Try to overpower a hostage taker unless a coordinated operation has been agreed.
- Try to escape unless it is the last option or you are 100% sure of success.
Wrongful detention

Individuals or government agencies may commit an illegal or wrongful detention.

To help avoid the situation

- Know the laws of the country you are in and do not break them.
- Find out if anything, such as alcohol, is banned.
- Avoid being drawn into any corrupt activities.
- Avoid doing or accepting favors.
- Avoid openly criticizing the country’s leadership, people or culture.
- Have the contact numbers of your national embassy.
- Use your diplomatic or personal in country contacts to identify trusted local government or law enforcement personnel.

If detained do not

- Resist arrest.
- Be abusive or argumentative.
- Try to bribe your way out of the situation.
- Do anything that could be misconstrued as evidence of your guilt.

If detained do

- Remain calm.
- Be patient.
- Explain there has been a misunderstanding.
- Suggest resolving the situation by sensible discussion.
- Claim your right to contact your national embassy.
- Ask to contact a colleague and/or lawyer.
About Hiscox in the US

Hiscox, the international specialist insurer, is headquartered in Bermuda and listed on the London Stock Exchange (LSE:HSX). There are three main underwriting parts of the Group: Hiscox London Market, Hiscox UK and Europe and Hiscox International. Hiscox International includes operations in Bermuda, Guernsey and the USA. Hiscox Syndicates Ltd is authorized by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority. The ability of syndicates at Lloyd’s to do business in the USA, and its territories, is restricted as they are not US-based insurers. Hiscox Underwriting Ltd and Hiscox ASM Limited are authorized and regulated by the Financial Conduct Authority.

Hiscox Inc., a Delaware corporation headquartered in New York, d/b/a Hiscox Insurance Agency in CA, is a licensed insurance intermediary for admitted and surplus lines business. Hiscox Inc. underwrites on behalf of, and places business with, Hiscox Insurance Company Inc. Other domestic insurers, and syndicates at Lloyd’s (www.lloyds.com). Hiscox Insurance Company Inc. (NAIC Number 10200) is a Chicago, IL domiciled insurer, which is admitted or licensed to do business in all 50 states and the District of Columbia. Inquiries as to insurance or other products or services should be directed to an insurance agent or broker licensed to conduct business in the relevant US state. For further information about an insurer’s ability to do business in the USA and US territories please contact a licensed agent or broker for advice.

This communication provides general information on Hiscox’s products and services only and is not intended to be, and does not constitute, a solicitation of business by syndicates at Lloyd’s from or in respect of the USA or US territories. Coverages are subject to underwriting and may not be available in all states. The information contained herein is not a part of an insurance policy, and may not be used to modify any insurance policy that might be issued. In the event the actual policy forms are inconsistent with any information provided herein, the language of the policy forms shall govern.

© Hiscox Inc. 2011. All rights reserved.