Incident Response Outline

Action steps on initial notification of a security incident or potential crisis involving individuals whom you advise

A. Note the source, contact information, and the exact date/time.

B. Determine what is known and what is assumed. Separate facts from assumptions to the degree possible.

C. Determine exactly who is involved in the situation (including dependents). Carefully note their current location and security status.

D. If follow-up communications with the source are necessary, determine the most secure means and agree upon an exact time.

E. Determine the location and status of other individuals you advise who are resident in areas close to the incident. Take all necessary steps to ensure that they are out of immediate danger. During this process it will likely be necessary to contact others. It is generally preferable to use non-written forms of communication for this purpose so that information cannot be easily passed along. Take care to let them know only what is necessary for their safety, not the details of what has happened at this point. Carefully instruct them to not pass along information to others. If applicable, let them know that they may need to relocate with little notice. Instruct them to calmly gather any essential items they will need and to begin destroying any documents that they do not wish to be accessed by others in the event that relocation is necessary. Let them know when they can next expect to hear from you, and what steps should be taken if they do not.

F. Determine exactly what decisions need to be made right away and at what point other decisions need to be made and by whom (see section 4 below).

G. Establish who knows about what has taken place. If necessary, ensure that all who know are instructed to not share any information until a communications plan is established. During a hostage incident or targeted killing, sharing information outside of a communications plan may result in the death of the hostage(s), or the killing of more individuals. It is especially important that email not be used unless absolutely necessary since email messages are subject to mass forwarding.

Follow-up steps to take after initial notification of a security incident or potential crisis

1. Begin an Incident Log
    - 1.1. Use the 24-hour time format to begin each new entry.
    - 1.2. Use a separate entry to record actions taken and each piece of information received.
    - 1.3. Include all phone calls, email messages, etc.
    - 1.4. Note decisions made and by whom in bold or with an asterisk for quick reference.

2. Define The Incident
    - 2.1.1. Describe what has taken place with as much clarity as possible.
    - 2.1.2. Where and when did the initial incident take place?
    - 2.1.3. Where and when have follow-up incidents taken place?
    - 2.1.4. What else needs to be known in order to make sound decisions?
    - 2.1.5. How can more information or more accurate information be obtained?

2.2. Determine exactly which individuals you advise are involved. Make a chart listing the following information for each individual directly impacted:

2.2.1. Their name.

2.2.2. Their spouse's name (if applicable).

2.2.3. The name and age of each child (if applicable).

2.2.4. The location and security status for each individual and dependent.

2.2.5. The contact information for each individual.

2.2.6. The nationality of (and passport # if available for) each member.

2.2.7. Any special medical concerns or medications for each individual or dependent.

2.3. Determine who else is involved in the incident.

2.3.1. Local partners working with or connected to individuals whom you advise.

2.3.2. Other agencies/organizations in the immediate area.

2.3.3. Opposition elements involved (i.e. governments, militant groups, etc.).

3. Contact the Appropriate Leaders

3.1. If the situation is a kidnapping, killing, or other incident in which the spread of information may put others at risk, ensure that each person notified is aware that no information may be passed to others, especially by means of email. Stress that doing so may result in the loss of life.

3.2. Make a list of the leaders within your agency/organization who should be notified of the situation, and kept updated. This should generally be on a need-to-know basis.

4. Determine who has Decision-Making-Authority

4.1. The outcome of an incident or crisis is often determined by the quality of decisions made, especially during the early stages.

4.2. It is vitally important to determine and clearly communicate who has Decision-Making-Authority (DMA) and for which decisions.

5. Develop a Communications Plan

5.1. Determine what information should be handled on a strictly need-to-know basis, exactly who needs to know, and how this information will be controlled. All need-to-know information shared must be clearly marked CONFIDENTIAL, with exact forwarding instructions and/or limitations included.

5.2. Determine what information may be shared openly. Consider developing an official statement if an internal and/or external (media, web, etc.) release is necessary.

5.3. Assign a Key Contact Person for individuals involved in the situation.

5.4. Assign a Key Contact Person for internal communications.

5.5. Assign a Key Contact Person for external communications.

5.6. Ensure that all parties are familiar with the communications plan and adhere to it.

6. Determine Whether an IMT or CMT Should be Established

6.1. It may be that only a few leaders need to be involved in the decision-making process surrounding the incident in question, and that the incident will be resolved quickly. In the event that more leaders need to be informed, or that more than a few days or so are likely to be necessary to resolve the incident, the establishment of an Incident Management Team (IMT) may be necessary.

6.2. An IMT is an agreed-upon group of leaders who are copied on email updates in relation to the incident. The incident should be given a title (i.e. Sudan) and each new email message should be titled in sequential order (i.e. IMT-Sudan-Update-11). Members of the IMT should use the "Reply to All" feature of their email client to respond to IMT Updates.

6.3. The distinction between an incident and a crisis and the establishment of a Crisis Management Team (CMT) is a formal process that needs to follow an agency/organization's written policies.

7. During Some Incidents, and During a Crisis, Leaders Should Consider the Following Options

7.1. Should Outside Specialists be Brought into the Incident/Crisis Response?

7.1.1. Tactical evacuation teams?

7.1.2. Medical evacuation services?

7.1.3. Crisis consulting specialists?

7.1.4. Hostage negotiation specialists?

7.1.5. Mental Health or Trauma Counseling specialists?

7.1.6. Media relations specialists?

7.2. Should Team or Individual Movements be Considered?

7.2.1. Sheltering in Place?

7.2.2. Should individuals separate or gather in one location?

7.2.3. Would in-country relocation be advisable?

7.2.4. Would relocation to a regional hub be advisable?

7.2.5. Would evacuation to a home-country be advisable?

7.3. Should an Initial Trauma Counseling Plan be Developed?

7.3.1. For individuals involved in the incident/crisis (by phone/email)?

7.3.2. Reception plan for those relocating or evacuating?

7.3.3. Debriefing resources?

7.3.4. Long-term care and follow-up?

7.4. Financial Considerations

7.4.1. What financial resources are available to assist in the incident/crisis response?

7.4.2. How will the costs of specialists be covered?

7.4.3. How will the costs of evacuations be covered?

7.4.4. Who will provide accounting for funds spent?

7.5. Crisis Management Center

7.5.1. At what point should a formal CMT be established?

7.5.2. Where will the CMT be located?

7.5.3. Will CMT members need to be co-located?

7.5.4. What resources (communications, direct lines, satellite news, etc.) are available?

7.6. Incident or Crisis Resolution

7.6.1. Who will manage the debriefing and lessons learned process?

7.6.2. How will the lessons learned be circulated and implementation responsibilities assigned?