WORLD TRAVEL & TOURISM COUNCIL

TRAVEL & TOURISM
SECURITY ACTION PLAN

AN ACTION PLAN FOR COUNTERING THE IMPACT OF GLOBAL TERRORISM

THE WORLD TOURISM & TRAVEL COUNCIL IS THE PRINCIPAL GLOBAL FORUM FOR TRAVEL & TOURISM BUSINESS LEADERS, COMPRISING THE PRESIDENTS, CHAIRS AND CEOS OF 100 OF THE WORLD'S FOREMOST COMPANIES.

The attacks of September 11, 2001 in the USA and other terrorist atrocities have highlighted an urgent need for a coherent strategy, based on a public-private sector partnership, to enhance the global security of Travel & Tourism. To address this, WTTC, together with leading security experts Objective Team, have developed an Action Plan aimed at coordinating efforts by all stakeholders, private and public, to reduce as far as possible terrorism's impact on the industry and its customers, and to strive for its ultimate defeat.

The Travel & Tourism industry is uniquely placed to address some of the issues that underlie the causes of terrorism. Its impact is felt at every level of society. The interface of peoples and cultures that it promotes contributes to greater international understanding and the wider tolerance of differences. Travel & Tourism can be the conduit by which prosperity can flow from wealthier to poorer communities, helping to address the imbalance between the 'haves' and the 'have-nots', particularly in areas where there are few alternatives for economic development.

The amorphous nature of terrorism dictates that the messages and methodologies incorporated within an action plan must remain flexible, retaining the capacity to adapt and evolve as the nature of the threat changes.

THE OBJECTIVE

This document sets out for the first time the WTTC Security Action Plan. After a brief summary of its context, it describes four key operating principles for those involved in or associated with Travel & Tourism. These are drawn from global experience of combating terrorism and can be applied generically at every level from the strategic to the local and across the public-private sector interface.

The plan is not just a collection of high-flown ideals. It extrapolates each of these principles as a series of practical measures that represent a framework for action. If widely adopted throughout the industry, internally and in its dealings with the public sector and customer, this checklist will help promote the universal methodology required when forming a coherent response to the challenges posed by terrorism on a global scale.

THE STRATEGIC CONTEXT - HELPING TO ADDRESS GRIEVANCES

Addressing the underlying or perceived grievances that enable terrorism to flourish is a major part in removing its threat. This must underpin all policy decision-making, the framing of security plans and procedures and the recruiting and profiling of staff, particularly those involved with security.

The constant and ubiquitous exposure and exchange that Travel & Tourism engenders between peoples of different beliefs, culture, race, politics and economic prosperity is unique. It can be argued that the manner in which the industry and its customers interrelate with those local people with whom they come into contact will have, for good or ill, *the* critical impact on the fight against global terrorism. The importance of this impact, and the need to ensure that it is beneficial, cannot be overstated.

Positive results, however, can only be achieved through an acknowledgement by all industry employees and customers that grievances do exist, and that their root causes need to be understood. Only then can appropriate policy guidance be given and action be taken to find remedies, though these must always reflect broader public-private sector strategy.

The burden of ensuring that security initiatives take account of local sensitivities must not be borne only by those directly involved. It is the responsibility of everyone in the industry, and demands close coordination with the public sector at every stage of enterprise planning, implementation and operation.

Careful research must be conducted, with the integral involvement of regional experts from the public and/or private sectors, to ensure that the ways in which businesses are developed and run do not exacerbate grievances by antagonizing local populations. Every facet of each enterprise must come under scrutiny - from the architectural design of its hotels, for example, to the manner in which its customers are encouraged to behave and interact with local people. Industry initiatives must always contribute positively to the moral and aesthetic well-being and prosperity of the local community.

A balance has to be struck, which may call for reduced short-term business advantage in favour of preserving industry credibility and harmony within a region. Decision makers must always ask themselves the question: 'how will this action be perceived?'

The public sector will always have the final say in plans to redress grievances within national frontiers. Where clear plans are at hand, the industry must coordinate its own initiatives with these wider strategies. But if regional governments flout the wishes of communities and exacerbate grievances in an attempt to attract Travel & Tourism investment, the industry's leaders must cooperate to persuade them of their folly, even if this results in short-term commercial opportunities being lost. It is critical that the industry is not perceived as contributing to such grievances. And if governments fail to acknowledge an obvious need for social change, the industry should similarly exert pressure for action.

Whenever an enterprise is launched its budget should include contributions to community projects. Preferably those projects should be unrelated to it so that its support cannot be construed as a direct effort to gain advantage. Again, the selection of suitable projects must not be at odds with wider public-private strategy.

Maximum employment opportunities must be offered to local people. If this happens, bonds will develop between the industry and the community that will enhance understanding, open a 'window' onto local thinking and potentially provide invaluable early warning of terrorist targeting. Investment must be made in regional training and exchange programmes to ensure that local staff members are recruited not just for menial jobs, but in the broadest spectrum of roles.

Similarly the industry must endeavour wherever possible to draw on local resources and markets. The perception, and reality, of the industry as a significant consumer of local produce and therefore a net contributor to the local economy will do much to promote goodwill.

At every level, managers must take responsibility for keeping their staff informed of key political, religious and environmental issues and developments. Specific briefing programmes must address sensitive issues affecting regions and localities. All employees must also be made aware of current global trends and their implications for security.

Ensuring that these messages are absorbed and acted upon is a primary function of leadership.

TWIN TRACK APPROACH

It has been said that terror, insecurity and Travel & Tourism cannot co-exist. Though this might appear logical, it does not reflect practical reality and is also unnecessarily pessimistic.

Though global terrorism is not a new phenomenon the attacks of September 11 have clearly raised awareness of its menace. Fear of further atrocities are unlikely to be allayed in the near future, regardless of what advances are made in what politicians have called the 'war against terror'.

WTTC has no desire to promote the unachievable - an environment in which Travel & Tourism is able to flourish devoid of *all* risk. There is no need for over optimism, for the resilience of the travelling public should not be underestimated. There is clear evidence that in the aftermath of recent terrorist incidents clients have tended to postpone, rather than cancel, their travel plans, and have proved remarkably determined to resume them once the immediacy of a threat has lifted.

The challenge therefore is to underpin this positive capacity for regeneration with pragmatic messages that are easy to understand and operating measures that are of real practical value in mitigating the effects of terrorism, whilst acknowledging it as a continuing reality.

In this context, WTTC advocates a twin-track approach:

1 Promoting, to all sectors of the Travel & Tourism industry and to governments, a coherent strategy of high-level messages and associated operating measures designed, demonstrably, to alleviate vulnerability.

2 Convincing the general public and industry employees of the reality that Travel & Tourism must co-exist with the risk of terrorism, provided that risk is mitigated.

ACTION PLAN

Every successful counter-terrorist campaign to date has adhered to a number of security oriented principles, by no means exclusively military, of which WTTC believes the four below can usefully be applied to Travel & Tourism as core themes. They are expressed here as generic messages employable at every level and across the public-private sector interface:

1
Coordinate all policy, actions and communications;

2
Secure operating environments;

3
Aim to deny terrorists freedom of action;

4
Access and work with the best intelligence.

These principles should complement broader political, economic and military initiatives currently being promulgated by governments and other international bodies in the fight against terrorism. It is imperative therefore that any industry initiative or operating measure derived from them marches in step with public sector plans, whether at governmental or local level.

Such cohesion can be achieved only through excellent communication between the private and public sectors and between companies within the industry. Where security is at stake there can be *no* room for commercial rivalry. This is a strictly non-competitive issue and requires stakeholders to work together, communicating freely with each other and adhering to the general guidelines promoted through this Action Plan. It is equally vital to 'humanize' security by teaching industry employees and members of the public to become more aware through

coordinated public-private programmes – 'fighting fear with knowledge'.

These principles run as core themes through the operating measures described below, which in turn must be tailored by stakeholders and their public sector colleagues to meet the differing requirements of each environment. Once so defined, however, all procedures and practices must be subjected to constant review to ensure that they remain relevant to the evolving situation, globally and locally.

1. Coordinate all policy, actions and communications

1a. In the development and communication of policy, leaders within the Travel & Tourism industry must engender a spirit of cooperation amongst their employees, and between them and representatives of governments and other organizations with whom they come into contact

Internal security policy and procedures must accord with and fully complement public sector policy at every level. In instances where a coordinated government plan either does not exist or lacks coherency, industry representation must be made at the highest level to rectify the situation.

From inception, project development and defining associated security policy must benefit, and be *seen* widely to be benefiting, from regional and local representation, both from within the industry and from external bodies such as government, local authorities, security agencies and other interested parties, including surrounding communities. The impression of security policy as a template imposed from outside must be avoided at all costs.

Therefore it should be an early priority to establish a Security Policy and Coordination Committee (SPCC) with broad membership and a schedule of regular meetings.

Security policy must develop in tandem with the overall commercial plan and should be proactive. There should always be security input to the making of commercial policy. Without a coherent security strategy already in place an evolving enterprise would be vulnerable.

To this end, an empowered decision maker involved with the development of commercial policy should have a seat on, though not chair, the SPCC.

The SPCC must include representation from the public sector. In order to reflect and contribute to the broader security strategy of a particular country or region, the committee may have to take direction from the public sector. Selected access for representatives of relevant pressure groups and media should also be considered when appropriate.

SPCCs must include public or private sector members with knowledge of intelligence procedures and a broad understanding of operational issues.

To be effective, security policy must be founded on a combination of the best technical expertise, drawn from the widest range of sources available, local knowledge and experience.

Therefore, the preparation and training of security policy makers and staff, as with all other employees, must be inclusive:

- regional or local security representatives must receive thorough grounding in the skills required to maximize the effectiveness of imported security doctrine, procedures and technologies; and

- industry representatives new to a region or operating environment must receive thorough education in its culture, social nature, politics, economics and any existing idiosyncrasies in the way Travel & Tourism functions there. Only in this way will the evolution of locally unacceptable or ill-timed security initiatives be avoided.

Inclusivity can best be achieved through global, regional and local exchange programmes within the industry and across the private-public sector interface. This will engender cross-fertilization of knowledge and experience, which is essential in breaking down barriers and building operational and cultural understanding at the local and personal level.

Regional and local authorities should be encouraged to participate in the running of internal security training programmes. Only by introducing public sector experts, concepts and procedures at an early point in the training of employees will a seamless interface be achieved - and a clear understanding of their responsibilities by both sectors reached.

Security policy must be succinct, unambiguous and straightforward in its application. Producing complex and lengthy policy documents will result in their messages being ignored or only partially applied - often more dangerous than operating in a doctrinal vacuum.

1b. *Coordinated actions for addressing security related issues must be developed by industry employees working closely with government and local authority representatives*

Security policy is not an end in itself. It is intended to give direction and credence to the development of doctrine and operational procedures - the tools of security staff, employees and customers – and to define the training and equipment requirements needed and the cost of successfully implementing them. In practical terms, policy, doctrine and procedure should form a 'cascade', enabling individuals at every level to access only those manageable elements of the whole that are relevant to them in their work:

- the greater proportion of all security procedures, perhaps as much as 80 per cent, will be broadly applicable whatever the particulars of circumstance or environment. These can be developed centrally and 'cascaded' from there to all employees as a matter of routine; and

- the remainder will be specific, either to location or threat, and will require detailed analysis of the governing factors in each case. Primarily this will be the responsibility of local security staff within the Security and Crisis Management Organization (SCMO - see below) working closely with industry colleagues and the public sector. But they will still need to liaise with the SPCC, as many procedures will have application elsewhere or might already have been developed to meet similar contingencies in other locations.

An internally or externally structured SCMO should be established. This should be subordinate to the SPCC. Its main responsibilities would be the development of individual action plans, the operational day-to-day running of security related activities and control in emergency situations. This additional tier, headed by a chief security officer (CSO), is required in order to separate policy making from operations. Experience has shown that combining these roles invariably creates an unwieldy, operationally inefficient body that can be slow to react.

The SCMO must reflect the same balance of public-private membership as the SPCC. It should have ready access to the SPCC, particularly in times of heightened threat, and both bodies should share at least one member in order to ensure smooth communication between the two tiers.

Public sector security agencies should be encouraged to assign liaison officers with security and intelligence expertise to the SPCC and SCMO.

Whenever possible the same representatives, from public and private sectors, should attend SPCC and SCMO meetings. This will encourage greater continuity and cohesion, stimulate stronger working relationships and establish trust.

Any security action plan must ultimately have a single 'owner', sponsor and controller. This is because in operational situations confused lines of communication and multiple points of contact will lead to confusion, which spells danger. Therefore, in matters relating to on-going or imminent security operations, the SCMO would take precedence over the policy-makers of the SPCC for the immediate duration of any incident.

It is key that all commercial managers and customers become subordinate to the CSO when such incidents occur or when the threat level is deemed high enough to warrant it.

Whenever possible, security plans should be designed to complement and replicate existing, proven structures and procedures. This reduces the time and money spent on training, limits scope for confusion and capitalizes on existing skills levels and knowledge.

Security action plans for every enterprise must conform and contribute to an overall strategy based on shared and clearly defined objectives identified in consultation with other industry members and relevant elements of the public sector. Neither the overarching policy nor the ground level operational security plans that derive from it must evolve in isolation - and a clear and regular system of communication must be established to ensure that this does not happen.

1c. *Clear and strong channels of communication must be established within the industry and externally with local representatives at every level*

Good communications are the single most important contributor to operational effectiveness in the security field. Without them the passage of intelligence, the key to formulating proactive policy and sound security procedures and systems, becomes impossible.

Responsibility lies with the public sector for ensuring that effective conduits of communication are established for security coordination. If these are not clearly apparent, the industry must lobby to remedy the situation, at governmental level if necessary. To proceed with an enterprise without first clearly identifying these points of contact would severely degrade its operational security and expose staff and customers to unacceptable risk.

Intelligence must flow in all directions:

ê

'downwards' - correctly disseminated information and direction must cascade from strategic or global policy makers at top, through regional to local levels, and from them to those responsible for security protecting each individual enterprise;

è

'sideways' - from the industry to its customers, who may well be first to detect a threat, engendering a two-way exchange of information at every level; across the public-private interface, both through formal channels and via 'informal' personal contacts, which must be assiduously cultivated by industry employees at every opportunity; and through close liaison across the industry, which is vital to reduce misunderstanding, eradicating the negative impact of competition and creating a culture of shared common practice;

é

'upwards' - because employees and customers at the local level will often be the first to pick up the signs that a threat is about to escalate the passage of information from grass roots upwards is of paramount importance. Senior managers must be open to comments and suggestion from below, and must ensure that information they receive is efficiently and rapidly disseminated.

The relative complexity of these flows of information calls for a clear communications strategy. Responsibility for this should lie in the first instance at the global policy level and should not be integral to the narrower security architecture. This is because many disparate factors such as marketing, sales trends and commercial goals will also have a bearing on the formulation of the messages to be communicated. However, the security input, especially that of intelligence, will have a major impact in defining the appropriate message to put out.

Therefore those responsible for the implementation of security must always be represented within the forum responsible for communications.

If the correct messages are to be sent, the information on which they are based must be up to date. Therefore, the bodies responsible must meet regularly - monthly at the strategic level, weekly at regional level and perhaps daily (or even hourly in times of crisis) at local level.

To be effective a message must be pitched at the correct level and delivered by a means that will engage the recipient. Globally, multi-media may be the best method but at local level the same message, adapted to suit the environment, could be better transmitted by local people, lending relevance and resonance to the information.

A standard event/incident reporting system should be developed within companies and, in due course, across the industry, to speed the passage of information and lessen the risk of it being misinterpreted. Wherever practicable these systems should reflect and be allied to formats and mechanisms used in the public sector.

A major focus of communications at the strategic level must be to influence the public sector, in three principal ways:

- to bring pressure to bear on governments and authorities to support industry-led security initiatives and take responsibility for relevant aspects of them, such as intelligence collation and analysis, for which specialist public sector agencies are specifically structured and funded;

- to persuade the travel advisory agencies of governments that they must refine the warnings they publish. Blanket threat levels currently applied to whole regions of the globe are not only harmful to the Travel & Tourism industry but highly counter productive for the longer term campaign to project a positive image in the affected areas and may encourage terrorists to believe their actions are having the impact they desire;

- to convince the general public and industry employees of the reality that Travel & Tourism can co-exist with the risk of terrorism, provided that risk is mitigated.

2. Secure Operating Environments

2a. The Public Sector must be encouraged to produce clear direction on the nature of the threat and the security measures required to defeat it

It is a government responsibility to identify and highlight areas of security concern within national borders and to set the broad criteria when establishing measures appropriate for general and specific threats.

Should government or other authorities fail in this duty, the industry must represent its disquiet in the strongest terms and at the highest level. It should demand at very least the production of a coherent threat analysis and an associated security checklist, which could be used by local authorities and the industry as a basis for planning.

2b. A comprehensive security plan is required to ensure the protection of the public and industry employees throughout every stage of an enterprise

The basis of creating a secure environment lies in the development of a sound security plan. Every enterprise must have its own, which must never be a direct template transferred from one scenario to another. Although many of the procedures and much of the terminology may be the same – and can and should be replicated for commonality of practice and ease of communication - individual applications will invariably differ, if only slightly. Applying a standard model and making the environment 'fit' it runs the risk of leaving gaps which an aggressor could exploit.

Therefore, each security plan should evolve from a formal and independent process of analysis, which must be undertaken by a trained security specialist, working closely throughout with industry

colleagues and adhering to appropriate guidance from the public sector. Ideally this guidance should be articulated in an effective certification process, as described above. The factors that should be considered in making this analysis will vary according to scenario, but the following are likely to be to the fore:

Threat - analysed in global and regional terms, but also with specific focus on local issues that may influence the immediate security climate and allow access to aggressors from outside;

Profile - careful consideration must be given to the impression that security measures will create within the local community. The ring of steel approach may seem an effective deterrent, but it could be entirely counter-productive, alienating the local community outside the ring or, worse, appearing to throw down a challenge.

Overt security does not sit comfortably with Travel & Tourism - customers want to feel secure, but they do not wish to be confronted by evidence of security at every turn. Any plan, therefore, must strike a balance, providing comprehensive security but in a manner conducive to the industry's commercial aims.

Use of technology - or the availability and suitability of technical security equipment and IT to meet the defined threat. Whilst the focused application of technology can greatly enhance capability, consideration must be given to the following:

- a structured programme of initial and continuation training for operators. Because equipment is only as good as its operator, emphasis must be placed on the aptitude of those earmarked for the role;
- maintenance of technical systems - specifically, ready access to specialist resources such as engineers and spare parts;
- the employment and management of technology as a contributor to an integrated security plan, channelling technical advantage to enhance, rather than drive, that plan;
- the potential dangers of complacency which can result from over-reliance on technology and which, if detected by terrorists, may be exploited by them. Technical capability must always be underwritten by alternative methodologies;
- the financial cost of technology, particularly in regions where no local technical infrastructure exists to support it.

These points should be taken into account during the certification process, which should include analysis of the most appropriate and efficient use of technology.

Human Resources - ultimately, the effectiveness of any security plan relies not on technology, but on the skills, commitment and aptitude of the people involved in implementing it. Therefore, in devising a security plan, careful thought must be given to the criteria governing the selection and training of security staff and other employees. To feel ownership of the system, which is vital, members of staff, particularly local people and those not directly involved in the security field, must be confident in their ability to perform their allotted roles.

Bearing in mind the confusion likely during most emergencies, the plan must be straightforward, easy to understand and tailored to the capabilities of those involved.

Public Sector Support - the plan must not conflict with regional or local initiatives, and clear delineation of private-public sector responsibilities, including control arrangements during crises, must be defined early in the process. This calls for close consultation with representatives of the public sector throughout the drafting phase. Subsequently industry security staff must draw on the public sector for its local knowledge and experience, and for specialist expertise in areas such as intelligence and technical support. It is important that these bi-lateral relationships are established at the earliest opportunity and are constantly maintained.

2c. Regular and independent reviews must be conducted to ensure that the relevant authorities and others are complying with the implementation of security requirements and are meeting their responsibilities fully

Once the security plan is complete, the CSO, who should ideally have assisted with its drafting, will take charge of it. It is his or her responsibility to implement it (through the SCMO, if one exists) and to ensure that it evolves to meet changes in threat as they occur.

To achieve this, the CSO must conduct regular reviews of all procedures, consulting widely

both internally and with contacts in the public sector to ensure that the implications of new factors such as emerging trends are covered by the plan.

The CSO must institute an on-going programme of continuation training for security staff and other employees, and a briefing programme for customers to keep them abreast of what they can do to ensure their own safety.

Security specialists from outside should also conduct periodic external reviews, aimed at confirming that plans and procedures remain relevant. These external reviews should include exercises designed to test the systems and, where possible, should incorporate involvement from both the private and public sectors.

The industry should have access to professional security support, in the form of crisis management teams which it can call upon in emergencies. These teams which should include specialists in intelligence liaison and operational procedures.

3. AIM TO DENY TERRORISTS FREEDOM OF ACTION

3a. Travel & Tourism enterprises must make contact with and engage as wide a cross section of the host community as possible, including those not directly affected by their operations

Without engagement – winning hearts and minds beyond the immediate confines of an enterprise - managers will have little feel for the prevailing regional and local ground currents, which are likely to be the first indicators of an increased threat.

Denying freedom of action to the terrorist is closely allied to the process of addressing the underlying grievances, perceived or real, simmering within local communities.

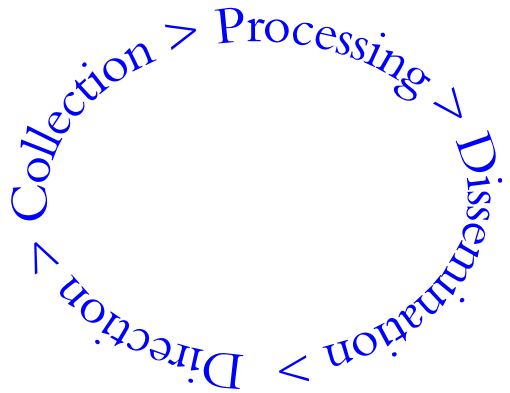
3b. Assessing the suitability of future employees

It is essential that industry stakeholders institute a system for assessing whether potential employees are likely to prove security risks.

4. ACCESS AND WORK WITH THE BEST INTELLIGENCE

Threat is defined as the product of an aggressor's intent, plus capability. Only by anticipating the former and neutralizing the latter can threat be reduced or removed. To achieve either requires access to good intelligence.

The gathering of intelligence, defined as the processing of raw data into usable information, must be subject to constant review and amendment as new information is received. It is best described, therefore, as a cycle:



The Travel & Tourism industry must develop a coordinated and structured approach to meet each of these four stages, exploiting to the full areas of internal strength, notably its in built capacity for the collection of local intelligence, and referring to the public sector in areas of weakness, such as the processing of that information.

4a. Direction

Industry leaders, especially managers in the security sector, must establish close consultative links with government and other public sector security agencies. Through this liaison current threat trends can be determined and internal intelligence collection priorities defined.

These priorities must be communicated through every level of the industry, and between companies, in a form and language that can be clearly understood by all employees, the great majority of whom will have no experience or training in security or intelligence, but who nonetheless have ready access to potentially vital information gleaned from customers and local contacts.

The impression that companies are trying to set up local spy networks should be avoided at all costs. It should be emphasized and re-emphasized that the intention is only to engender straightforward awareness amongst employees of what constitutes information which, when processed, could contribute to the building of an intelligence picture by public-private sector security professionals.

4b. Collection

The global reach of Travel & Tourism provides a superb framework for the collection of information. Capitalizing on this potential not only offers the industry an opportunity to contribute to international counter terrorism efforts but by providing information to public sector agencies also allows access to processed intelligence in return.

To facilitate the subsequent efficient and timely processing of information, the industry must have systems for verbal and written reporting. The responsibility for compilation should fall to the CSO. Reports should be framed using a common format and terminology, and should be delivered according to a fixed schedule or, in the case of high priority information, at the earliest opportunity.

Within each company there must be a single focus or conduit through which all collected information should pass before being committed to processing (probably by the public sector). To maintain a seamless interface between security operations and intelligence this role should belong to the SPCC, or a sub-committee of it.

The strength of the Travel & Tourism industry lies predominantly in the field of intelligence gathered by human contact. Technical methods, such as the use of IT to survey manifests, can supplement this but never supplant it.

4c. Processing

Processing consists of the collation, evaluation and interpretation of raw information and turning it into usable intelligence.

This task is usually undertaken by professional intelligence analysts, though not exclusively. For instance, low level intelligence relating to individual enterprises at the local level is best processed and disseminated locally; processing staff with no intimate local knowledge or experience of the operating climate would very likely miss some key nuances. Therefore, for this type of immediate intelligence analysis, it is incumbent on local security managers to create their own liaison and processing links within local community and public sector agencies.

For the bigger picture, however, the industry must rely on the services of high level intelligence processing structures in the public sector. To attempt to replicate these internally would not be financially cost effective and would require structures and pools of experience and expertise that can take years to establish. Public sector security and intelligence agencies that, in this context, could include certain commercial security companies specializing in intelligence, are geared for processing. The Travel & Tourism sector is not.

Therefore it is critical to open effective and timely avenues of communication across the public-private sector interface, so that raw information can be passed one way, and processed intelligence the other.

4d. Dissemination

The best intelligence is rendered useless if it fails to reach the correct user in time. Dissemination relies on the same principles and procedures of fluid communications already described.

The intelligence product should be quantified in a straightforward risk matrix, colour-coded for simplicity. For ease of communication, it may be beneficial to adopt public sector threat categories, although these tend to vary.

Each grade of threat should trigger an appropriate security response, according to the procedures laid down in the security plan.

Close liaison between the public and private sector at every level is needed to ensure that threat messages, disseminated internally within the industry and externally to the wider community, are never at variance with one another. A failure in coordination could lead to confusion and an inadequate response at times of heightened risk.

As processing capability lies predominantly in the public sector, that sector must be encouraged to take responsibility for disseminating such processed intelligence as is relevant to the industry, and in the timeliest manner possible.

This could best be achieved through regular coordination meetings, hosted by the public sector, at which industry stakeholders could be briefed on the latest security situation and intelligence developments affecting their enterprises.

These meetings could also provide a conduit for passing on information collected by stakeholders to the authorities for processing and wider dissemination.

UNIFYING STATEMENT

These four principles are mutually supporting. In developing security policy, adherence to all of them is essential if the sum of the product is not to be weakened in a way that will allow the appearance of gaps that terrorists can exploit. However, they are essentially a response to terrorism, rather than a solution.

The industry already possesses much of the infrastructure needed to gather and disseminate intelligence that can counter the menace. Through their established commercial networks, with the associated capacity for highlighting regional and local issues and exerting beneficial influence, companies can make a fundamental contribution in the campaign to eradicate global terrorism altogether.

WORLD TRAVEL & TOURISM COUNCIL
1-2 QUEEN VICTORIA TERRACE. SOVEREIGN COURT. LONDON E1W 3HA. UNITED KINGDOM
TEL: + 44 (0) 727 9882 OR + 44 (0) 207 481 8007 FAX: + 44 (0) 870 9882 OR + 44 (0) 207 488 1008
EMAIL: enquiries@wttc.org **WEB:** www.wttc.org