



September 2005

Addressing national security misconceptions is critical in developing effective public awareness campaigns

As governments contemplate the next security awareness campaign, it is time to provide the target audiences with much more sophisticated content. Past campaigns were appropriate at a time when the security threat was new, but the audience is now more segmented and better informed

What is required is a campaign aimed at the general public which builds on the two past public awareness campaigns, plus a second campaign aimed at engaging the business community.

This is because the business community is thirsting for more detailed information about their roles and responsibilities, and how they can be engaged.

There are two critical elements in future campaigns. Firstly, a call to action stating what is actually required of the target audience, and secondly, messages which neutralise incorrect perceptions that prevent people from accepting and acting on the awareness message.

The purpose of this *National Security Practice Note* is to flag issues which are currently undermining national security awareness campaigns aimed at the public or business community. These misunderstood issues undermine trust in the government, reduce motivation for taking action, and can make

National Security Practice Notes is a publication series that covers topical issues which are of critical importance to building national and domestic security capability. They are aimed at practitioners in the intelligence, security, law enforcement, emergency services and related national security areas.

individuals feel powerless. They must be addressed so that people take security threats and their responsibilities seriously and actually contribute to the nation's security.

The issues which need to be addressed relate to misconceptions about risk management and intelligence.

The issues which need to be addressed relate to misconceptions about risk management and intelligence.

The first misconception relates to the nation's fundamental response to terrorism. This response is based on risk management, which means that resources are allocated on the basis of the threat and vulnerability (alternatively viewed as likelihood and consequences).¹ For example, applying a risk management approach results in all hand luggage at capital city airports being screened because it will generally be loaded into large jets, with catastrophic consequences if a weapon is smuggled onboard. Conversely, at small regional airports, passengers' luggage is rarely screened as these people fly on smaller planes and the consequences of an incident would be much less. However, many people hold the misconception that the nation's response is based on risk elimination, meaning that all risks are eliminated. In the case of luggage screening, this means that they expect all luggage to be screened regardless of the relative risk. Implementing a nation-wide risk elimination approach would be both impractical and financially unviable.

The Australian Homeland Security Research Centre undertakes independent, evidence-based analysis of domestic security issues.



National Security Practice is a publication series that covers topical issues which are of critical importance to building national and domestic security capability.

National Security Practice is part of the research program of the Australian Homeland Security Research Centre.

Athol Yates
Australian Homeland Security Research Centre
Tel 02 6161 5143, Fax 02 6161 5144
PO Box 295, Curtin ACT 2605
info@HomelandSecurity.org.au
www.HomelandSecurity.org.au

Copyright 2005. All rights reserved.

The second area of misconception relates to intelligence. While people generally understand that the first line of defence is intelligence, they do not understand the difficulties and complexity of the intelligence process. In particular they do not understand the difference between strategic and operational intelligence. Consequently, when a camera crew gets a tour of a purported terrorist training camp in the southern Philippines, the news story create an impression that intelligence is readily available if one just looks for it. However, while this strategic information may be of some use, it has no bearing on the operational intelligence required to identify potential terrorists in Australia who may operate in tight, independent cells, are dormant for long periods, use many aliases and communicate informally. This sort of intelligence requires both considerable information and analytical ability to build links between elements of data. To counter this misconception, effort is required to explain the role of intelligence and in particular, the role that individual pieces of information can provide.

A related misunderstanding concerns the difference between intelligence leading to the identification of “persons of interest” and information for criminal

prosecution. People need to be educated about the difference and that there are other effective ways to remove potential terrorists or sympathisers besides prosecuting them under counter-terrorism laws. Just as the US mafia in the 1930s was destroyed by tax evasion prosecutions rather than on racketeering charges, today’s potential terrorists may be neutralised by prosecuting them for visa violations or identity fraud rather than conspiracy to commit murder.

Another misunderstanding relates to the perception that governments are withholding from businesses vital intelligence about threats to their assets. The message that intelligence relating to a specific asset will be passed on very quickly has not been received by businesses.

The final misconception relates to the idea of ‘intelligence-driven threat assessments’. While threat assessments need to be based on intelligence grounded in the adversary’s capabilities and intent, there is a misconception that actionable intelligence is the only sort of intelligence that business should act on. The underlying incorrect belief is that there will always be intelligence of an impending attack. A dangerous extension of this perception is the belief that business does not have to respond to threats until actionable intelligence is provided.

Conclusion

If Australian governments want to transform the public and business community into another barrier to terrorism, people must have the facts about the nation’s risk approach and the limitations of intelligence. While past security awareness campaigns were appropriate for their time, future ones need to be more sophisticated and correct the widely held misconceptions that are currently undermining the population’s participation in national security vigilance.

¹ Technically inferring a direct relationship between threat and vulnerability and, likelihood and consequence, is incorrect. Risk is measured in terms of likelihood and consequence (severity) while risk equals threat divided by vulnerability.

Security Jobs Central

Positions for security, risk and intelligence professionals

Sign up for your free weekly email listing positions vacant at
www.securityjobscentral.com.au

