Case Studies

Intelligent Outcomes Group (IOG) was commissioned...

…to conduct **Port Security Assessments** and produce **Port Security Plans and Port Facility Security Assessments** of several ports, in accordance with the International Maritime Organisation (IMO) International Ships and Port Security (ISPS) Code and the Maritime Transport Security Act in Australia.

…to provide ongoing **threat and risk management support** for the protection of port infrastructure and port operations. This involved a Port Security Assessment, a Threat and Risk Assessment (TRA), a security risk management methodology to support the implementation of proposed IMO legislation, and development of a draft Port Facility Security Plans in accordance with proposed IMO ISPS Code and Commonwealth legislation. Extensive consultations were conducted with key members of the maritime community, law enforcement and security agencies, and governments at both state and commonwealth levels. Security inspections and audits were also required.

…to develop **a whole of government risk management approach to critical infrastructure**, including a maritime emergency response capability, regarding potential terrorist threats. Departmental compliance with State government mandated risk assessment requirements within the infrastructure portfolio (ports, marine and land transport). There were consultations throughout the State maritime environment – including all major and most regional ports, maritime services operators etc. – regarding issues confronting the State's maritime emergency response capability. The scope included maritime threat events arising from potential attacks and the full range of maritime accident scenarios. Desktop review of risk assessment work was undertaken and consultation on gaps and weaknesses was completed.

…to provide a **Business Continuity Management Plan** and conduct **emergency response simulation exercises**. This required extensive consultations with key members of the maritime community, law enforcement and security agencies, and governments at both state and commonwealth levels, to develop comprehensive threat and risk assessments, and conduct the simulation exercise.

...to **review aviation security** at an International Airport against international standards. The review assessed all security factors including the communication and intelligence-system linkages between airport security staff and government stakeholders and retailers. We were able to draw on our intelligence background to provide realistic assessment of the intelligence processes and identify changes to its supporting infrastructure.

…to conduct a **Threat and Risk Assessment** and review of aviation and general security aspects of a regional airport, including a Threat and Risk Assessment to **ASNZ 4360:2004** on airport operations.

…to conduct a **Security Review** of corporate offices in a capital city. The task required a **Threat and Risk Assessments** of all domestic offices to identify all physical threats, consequences, risks, and preventative controls. The outputs of the Threat and Risk Assessments were used to produce a **Departmental Security Plan** and provide ongoing security and intelligence advice to the Secretary and senior management team.

...to provide ongoing **threat assessment advice** and periodic reporting for a client's operations in Australia, New Zealand, and Fiji. The reporting required us to utilize our range of associates and contacts in intelligence, security, and law enforcement agencies in Australia and throughout the Asia – Pacific region. Reporting included a monthly intelligence assessment of potential threats to the client's operations and immediate reporting of imminent threats via Special Alerts.

...by several multinational companies to **develop and maintain a series of specific geopolitical reports** on a wide range of countries in the Asia – Pacific region. The reports are used to inform each client's strategic business decisions in country and to provide early warning of any deterioration in the business and tourist environment.

IOG was commissioned to…

...to implement **Business Continuity Planning (BCP)** in a client's organisation. The task required us to develop an acceptable methodology for the client that supported its business processes and then build both corporate and business-unit level structures and documentation.

...to develop and implement a **comprehensive business intelligence process** for a client. The process required us to monitor a range of global competitors and provide early warning to our client of threats and business opportunities.

...to undertake a **sensitive review** of a specific industry for a government department. The review required us to develop a detailed understanding of the industry, its major players, and their linkages outside the industry. The review provided the client with a strong analytical basis against which to gauge the impacts of its legislative changes on the industry.

...to support a review into the **security of electronic documents** within government. The review required us to assess the current security of electronic documents across government, to identify the type and level of threat posed to these documents, and to propose a range of integrated and appropriate security countermeasures to be implemented by all government departments and agencies. In identifying appropriate countermeasures, we played an important role in helping to develop initiatives that changed the perspective of many departments and agencies on security and its part in supporting the achievement of their business outcomes.

...to undertake a comprehensive set of **penetration tests** of a client's physical and information technology infrastructure. The tests allowed the client to identify it's vulnerabilities and implement changes that significantly strengthened its defence against unauthorised access.

...to undertake **Threat and Risk Assessments** for several major government departments on their **Local Area Network** (LAN). This required identifying departmental elements to be included in the TRAs, then identify and evaluate the threats potentially confronting the LANs. We utilised our relationships with the appropriate security agencies, and our business relationship with the Australian Computer Emergency Response Team, to identify realistic potential threats and develop effective countermeasures. The TRA process also required us to facilitate an agreed assessment by departmental senior management of the acceptable levels of harm and required risk.

…to conduct **performance monitoring and audit arrangements** of emergency communications (emergency call taking and dispatch). Identify areas of overlap and gaps in current performance monitoring and audit arrangements and where appropriate make recommendations on these matters.

...to support a client's Year 2000 Millennium Project. Our charter was to **establish an early warning capability** to protect the client from Year 2000 related impacts by collecting information and monitoring Key Indicators. We developed and established an Information Monitoring Cell and information management process within the client's existing crisis management structure. Due to the success of the project, we were further contracted to incorporate the new procedures into its existing crisis management policies and procedures.

…to complete a **security risk assessment** for a Commonwealth department on aviation security onboard domestic aircraft and in regional airports.

…to develop a **Project Development Design** for an Australian Government Department looking to undertake a maritime anti-terrorist infrastructure project in Asia.

…to complete a **security gap analysis and security threat and risk assessment** for a large prestige residential and business development in capital city.

…to complete a **counter terrorism gap analysis** and develop a range of security threat and risk assessments for a major global city.

IOG was commissioned to…

…to undertake International Maritime Organization International Ship and Port Facility Security Code **capacity building** within the Philippines and Indonesia. The work also required us to develop security measures within the domestic ports and across land and rail and aviation infrastructure.

...to undertake a comprehensive **security review and then develop a security threat and risk assessment** for an electricity distribution company in Australia.

…to develop and implement a **security risk management methodology** for a government department responsible for several crowded place venues.

…to develop a series of **threat and risk assessments** for crowded place infrastructure in a major capital city.

…to develop a **threat and risk assessment** for an Australian state government health department.