



Risk Management and Assessment Workshop for Critical Infrastructure Protection

28/29th November 2005, NSW
Summary of Outcomes

1.0 Workshop Objectives

The objectives of the RNSA Two Day Risk Workshop were to develop a strategic research plan for security risk management in Critical Infrastructure and provide a networking forum for the development of collaborative research projects between researchers, industry and government.

Industry, government and academics presented their viewpoint on risk management and assessment for critical infrastructure protection and allowed showcasing of the current research work in this area, through forum sessions.

The targeted Workshops allowed the range of people to divide into close working groups, to openly debate current issues, requirements and ongoing work required.

This summary paper details the target workshops, including objectives, discussion development and overall agreed outcomes at the Workshop close.

2.0 Summary of Key Outcomes RNSA Risk Workshop

Risk Workshop Key Outcomes

- I. RNSA needs a strategy, business plan and marketing plan.
- II. RNSA needs to improve communication to all organisations.
- III. Better communication methods and practical tools are needed by SMEs and smaller critical infrastructure players, who do not have the resources of larger organisations to obtain information/assistance.
- IV. More work needs to be conducted on risk assessment, resilience, vulnerability and interdependency modelling, tool development and case studies utilising these tools.
- V. More work needs to be conducted on risk assessment, resilience, vulnerability and interdependency modelling, tool development and case studies utilising these tools.
- VI. Investigation needs to focus on whole systems and resilience of systems, not just individual organisations.

- VII. Investigation needs to focus on whole systems and resilience of systems, not just individual organisation.
- VIII. More joint projects are required between industry and researchers.
- IX. Requirements for further interaction and feedback with TISN and other groups.
- X. Greater support for researchers and opportunities to showcase and share work is warranted.
- XI. Confirm international body of work and applicability in Australia.

Risk Workshop Summary of Specific Research Needs

- I. Resilience - what is it, how do you measure it, and how do you achieve it in business, communities and infrastructure and total systems.
- II. Development of new risk assessment tools that cope better with non linear systems and critical infrastructure interdependencies, including supply chain interdependencies.
- III. Methodologies to aggregate risks and interlink risk management plans.
- IV. Communication and knowledge management issues prior to, during and after a disaster and communication needs at a tactical level during emergencies.
- V. Application of complex systems theory (and domino effect and butterfly effects and feedback loops).
- VI. Acceptable risk and risk perception in the security context. The balance between security and freedoms, individual and societal risk.
- VII. Development of methods for perceived risk in parallel to objective methods.
- VIII. How security threats can be incorporated with other risks that CIP businesses have to deal with in an integrated system.
- IX. Critical review of risk management products and tools used at present.
- X. Characteristics of organisations and teams needed to operate effectively in emergency situation - the role of emergence in effective emergency management.
- XI. Adaptive capacity of human and engineering systems.
- XII. Development of enabling low cost technology to assist in information and knowledge management and proactive response to developing circumstances.
- XIII. Motivation is poorly understood and requires development of metrics and new tools.
- XIV. Development of new methods for risk assessment of value correspondence that take account of the values of diverse social groups.
- XV. Communication of risk particularly to the public during a period of heightened threat and response.

- XVI. Post remediation studies of perception
- XVII. Research on whether addressing core factors such poor governance, shortage of political, economic and education opportunities, denial of civil liberty and gender inequality could mitigate conflict generating frustration and despair.
- XVIII. Studies of current conflicts to ascertain the degree they inhibit meaningful discussion in government and political decision making, better education opportunities, wider economic choices and improved standards of living
- XIX. Studies of successes and failures on how cultural and religious intolerance between and within peoples can reach or foreclose common ground.

3.0 Target Workshop 1 – Techniques for Risk Management and Assessment (threat, protection and response)

3.1 Target Workshop 1 Objectives

The objective of target Workshop 1 was to discuss the issues raised in the forums and specifically look at:

- Information gathering and use
- Risk Assessment frameworks and tools
- Meeting Industry and Government requirements
- Fostering Collaboration
- Increasing knowledge and skill in Industry and Government

The target Workshops were coordinated by attendees dividing up into areas of interest, in relation to threat, protection and response. The individual groups then presented a summary of discussions and outcomes to the full Forum session.

3.2 Target Workshop 1 Discussion / Comments

THREATS GROUPS

Discussions from the groups assigned to look at “Threats” are set out below:

Target Workshop 1 – Discussion Points – Threat Groups

- Concern that the right information is not getting to the right place at the right time – how do we ensure flow of information to users.
- Information management systems – are they effective. How are they being used.
- Use of information – quality of information and analyses, trends, target groups, how can we assess what is out there - research on information metrics
- Social and other network analysis – need to understand work done in this area

- Communication needs to be improved between the public, governments and public bodies and the private sector
- Research – knowledge management - what knowledge is used internally – how could that knowledge be used more universally
- What could government bodies provide to business.
- Intelligence agencies need to be aligned with business and have a willingness to share information.
- Industry continues to do its own research, as they cannot rely on government to pass funding through. Options outside formal government channels?
- Need central learning environment – combine agency, business and academics to collectively seek information at centralised location.
- Quality of information and risk management tools provided by consultants needs review. Research could be undertaken on the quality of services by consultants. Mapping consultant types and client types and differentiating them.
- What is acceptable risk? Research could focus on freedoms, law, reality, media portrayal, public needs and perceptions – balancing the different competing interests may change the balance of risk – a difference between risk to the individual and risk to society
- There is a need for more commitment, co-operation, response and communication amongst all players.
- ASIO has a problem with lack of responding – no one is responsible
- Key people in CIP's find they get lost in the system. Business groups don't have a huge amount of time to find their way through myriad of government information and assistance – need easy access to information and quicker responses.
- If industry do not have the same connection, they do not benefit from the information and knowledge out there. Players further down the “food chain” as compared to major CIP players, have difficulty getting access to information and lose confidence in what the current practice is.
- Need for development of seamless information gathering, dissemination and analysis systems to service the needs of industry to make appropriate risk management decisions.
- Research on how security threats can be incorporated within other risks that CIP businesses have to deal with – does it require compliance, ignoring or active participation
- Research on how dual purpose technologies can be controlled while ensuring economic development
- Need for international agreement and legal codes

PROTECTION GROUP

Discussions from the group assigned to look at “Protection” is detailed below:

Target Workshop 1 – Discussion Points – Protection Group

- CIP needs to consider the following issues:
 - Base line security measures
 - Common Language
 - Suitability of technology
 - Urban planning and CIP collation
 - Management
 - Built environment
 - Principles
- Some work has been done on systems, but gaps need to be identified.
- Dealing with mass gatherings has slipped through the cracks for some time. Work needs to be done in this area.
- Multi tenants in one building is also a problem to deal with. Difficulty in control of security of other entities outside your domain.
- Heritage, access to disabled and security – areas requiring further investigation.
- Communication and ease of flow of communication and how do we measure.
- Social decision making management and governance should also be addressed. There is a greater need to promote into organisations improved methods of management decision making. Investigate if support models similar to development of OH&S legislation are feasible or are there other frameworks that would be more suitable.
- Risk management and assessment - look at the range of products available to end users. Products need to be designed to meet potential threat and meeting risk assessment requirements or from regulatory compliance.
- Disparity in design between consultant versus organisational view. Greenfield products can't be tested. Work with ASIO, too expensive to test. Clients can't bear the cost of testing.
- Issues faced by a Vendor supplying security. Expectations of buyer not fulfilled. Look at how to solve these matters, very broad range of issues required to get the solution.
- Critical infrastructure protection includes non security risks including aging infrastructure
- Consideration of how resilience can be incorporated into design and the need for guidance material on how this can be achieved
- Development of rapid detection and identification of developing threats for protection and response.

RESPONSE AND RECOVERY GROUP

Discussions from the group assigned to look at “Response and Recovery” is detailed below:

Target Workshop 1 – Discussion Points – Response & Recovery Group

- Parties from different backgrounds and areas produce diverse input and solutions.
- Need to set up options for groups to exchange experience. As a minimum – share experiences.
- It is too late to wait until incident occurs to get collaboration and sharing – overcome obstacles and apathy.
- Management teams, being able to operate in a non routine environment, what are characteristics of organisations and teams needed to operate effectively in an emergency situation . How to achieve the required flexibility
- The role of emergence and complexity in effective emergency management
- Information flows are critical. Communication in an emergency is a non routine environment, traditional ways won't work. Failures in communication have often played a part in past disasters. Boundary issues – public sector, work on response and recovery at the community level, industry except Major Hazards Facilities do not. Boundaries shift and people in business will be working with sections of public sector more. Trust and relationships important
- Communication to the General Public prior to and during an emergency and the need to counter confusing, inaccurate and contradictory information
- Development of multi faceted information systems for seamlessly integrating real time data required to manage incidents from various command centres
- Activities need to promote working together.
- “Asymmetry” is a good motto for doing work in response and recovery.
- Decision making, needs informed risk management
- The RM Framework is there, but need a common language and understanding in the emergency area.
- Systems also need to be design to be resilient, not just business or organisations, i.e. reusable economic capital. Reuse aspects of the system after the collapse – so Intellectual property will grow.
- How does one measure resilience in systems communities and business?
- Adaptive capacity of human and engineering systems
- Need to move beyond system resilience to sector and societal resilience for overall approach in industries
- Industry groups, not always working effectively to communicate to members. Put in time and get progress occurring.
- Need a champion to make it happen, leadership and commitment.
- Whole of life cycle needs to be approached. Understanding the whole cycle and

all organisations involved.

- Good projects need to flow and co-ordinate involvement. Something positive in the form of projects should come out of it. Need something specific.
- Perception of threats - needs clearer definitions
- Explicit point – success of response and recovery, will be preparation for the unknown. Other detailed planning.
- Development of best practice guidance for mitigation on the general public – curtailment of rights, control of movement, quarantining, treatments and decontamination
- International agreements on cooperation, degree and type of assistance for specific threats and hazards
- Development of simulation techniques that approach the intensity and conditions of an actual event
- Technologies that are adaptable to multi hazard environments
- Discussion on how to invest resources across all political jurisdictions
- Development of low cost, highly efficient and reliable, lightweight barrier technologies that can be used for a broad range of challenges.
- Development of real time smart tracking systems for responders and victims
- Novel technologies and system engineering for new generation of integrated detection systems that can identify hazard and relevant environmental data, determining the extent and likely progression, be low cost and robust, accurate and take advantage of modern global communication systems

4.0 Target Workshop 2 – Gaps and Needs

4.1 Target Workshop 2 Objectives

The objectives of target Workshop 1 was to develop a consensus as to what research should be undertaken and specifically look at:

- Governance and management
- Vulnerability, interdependency, tools and techniques
- Communication by researchers, industry and government
- Setting the future direction for this network

The target Workshops were coordinated by attendees dividing up into areas of interest, in relation to Governance and Vulnerability. The individual groups then presented a summary of discussions and outcomes to the full Forum session.

4.2 Target Workshop 2 Discussion / Comments

VULNERABILITY / INTERDEPENDENCY GROUP

Target Workshop 2 – Discussion Points – Vulnerability / Interdependency

- Wide and varied discussion. Focus on vulnerability and interdependency.
- Common definitions and assessment of vulnerability are required for better understanding and consistency.
- Communications – we need to map the way communication flows and how to interface into other organisations.
- Threat notification service. The information is there but it is not getting to organisations, even short term notice Quality and timeliness of information
- Organisations want more information to use in development and decision making process.
- Need work on interdependency, domino or butterfly effect and modelling, including particular activities with outsourcing, make sure we understand effects.
- Further testing of plans and systems, how are they going to work? How effective and robust are plans and systems.
- Need less linear risk management strategies and approaches, perhaps in a better format.
- Aggregate risk management plans; don't need each organisation's full plan, just key components to be shared.
- Need for further understanding of what work has been done overseas and who it could be useful for. The assessment needs to be made.
- Research overlaps into the social science area. Resilience of community and people and this comes into assessing risks.

GOVERNANCE / MANAGEMENT GROUP

Target Workshop 2 – Discussion Points – Governance / Management

- There is a disparity between researchers and industry understanding.
- You need a clear communication plan, is it CI versus major industry, good information needs to get through to all organisations.
- Need a communication and marketing plan. Fed govt have pushed us towards looking at this. How do you go about presenting your case?
- Need to look at Federal and state. Website overseas provides hyperlinks to research boards. Overseas look more engaged and screening of subjects for CI. We need co-op research boards. 9 sections for CIP are well known. What is an

Australian Equivalent to work towards?

- Conflict between consultants and academia and the services that each can provide. US are doing lots of research.
- What do you want to provide, marketing plan needs to set this out, reduce the need to get the research being done privately.
- Fed govt wants academics to interface with industry. Fed govt function through ARC and Health, competitive grants, 20% for pure research and there is a time delay – long lead time. Can't get important discoveries out in to the commercial world. Incompatible timescales for federal funding and the requirements of industry
- Monash – have not had the link with industry yet. People discover each other by chance and its difficult to interact.
- One problem we haven't talked about is that this is a very sensitive area which govt. is attempting to address. Have to factor this in the way you have dialogue. TISN have struggled with confidentiality.
- Business Resilience should be a major research area.
- Tie into the IAAG's. TSIN is 12 months in front of this group. You can do presentation to IAAG; meetings are bi-monthly.
- You don't need to be a member to communicate with IAAG. They need to have input. It is an open system.
- You can make presentations to each group.
- AG should feed back to RNSA.
- Need a media Champion, communications plan.
- More information exchange. More strategic groups, but needs to filter down to all organisations at all levels.
- Concentrated on what are the barriers to us moving forward. Neutral areas of relevance to industry and academics.
- We need a communication plan to communicate to industry what topics researches are interested in the area and feed back too all levels on the food chain.
- Need for exchange of live projects and building of trust between both groups.
- Communication plan, articles in the newspapers, showcasing of work done, and the process on the map. Resilience is the common point of reference, particularly in CIP it is a key issue, aging, economic probs. Look at environment and building resilience. Go out with a proposal to stimulate discussion, with a marketing plan to compliment. Seek out and engage. Don't be passive. Have a plan.

5.0 Overall Discussions and Summary at Close of RNSA Risk Workshop

The overall discussions and comments in general agreement by the all attendees are listed below.

RNSA Risk Workshop – Summary of Discussion at Workshop Close

- RNSA needs to facilitate improved communication between academia and industry. Needs a communication and a marketing plan
- Plug RNSA people into TISN.
- Look at futures and application of future studies research in risk assessment
- Get RNSA presentations at futures group and at security conference
- Short sharp workshops are what is needed, with research topics that are relevant. Feed in filtered material coming from specialist groups.
- Resilience is what is needed in the future. Society depends upon this fragile system, hence it needs to be teased out. We need to speculate. Not sufficient to be just responding to incidents, or responding to what is happening overseas.
- In academia, in order to progress you need to be a specialist. So we want TISN to find out what everyone does and let us know
- Projects RNSA decide to progress with, people hear for different background, we are all interested in getting involved. They are not all going to do research. Get interaction.
- We would like to get a much broader coverage of industry.
- RNSA – needs to market to TSIN – need govt and private reps from each of the 9 groups.
- Reverse engineering, tell us what work we need to do by industry and government??
- RNSA Steering committee should be an aggressive driver.
- If organisations had someone high profile in the industry as the media front – futures groups, presence needed. High profile champion.
- Mechanism for industry to get access to smart young people, and consultants - CSIRO have access to it. CSIRO are a networking interface between industry and research in a commercial sense. Eg Links on the website, find a researcher. Rapid response is needed.
- Break down pockets of isolation. We need an information pack on the web which I can download and send to my colleagues.
- You need some RNSA marketing information.
- RNSA should showcase what PhD students are doing.
- Industry – want scholarships for PhD students.

- PhD pathway should harvest the information we need.
- TISN – intention was a representative group who would represent all expectations and views.
- RNSA should be a hub – get a network of people you can talk to about problems/issues.
- Industry does not understand what RNSA are about.
- Need to also showcase what universities have – like overseas web sites citing expertise.
- RNSA – draw in all those PhD projects that require funding, here is a list of avail scholarships and the ones running
- In UK you often have multi sponsored research - opportunities to do this here.

At the close of the RNSA Risk Workshop it was agreed to document the workshop outcomes, as provided in this document, and distribute to all workshop attendees for comment..

The next RNSA Workshop topic and date will be advised in early in 2006.

RNSA thank-you for your attendance and valuable participation and input in the risk workshop.

Prepared by: *Priyan Mendis*
 Colin Duffield
 Collette Burke
 Tony Green
 Jean Cross

December 2005