

Critical Infrastructure Protection and Security Forum

Prepare, Respond and Recover - working together towards a holistic system resilience

Swissotel Sydney

11th & 12th June 2009

"The best we can do is to size up the **chances**, calculate the **risks** involved, estimate our **ability** to deal with them and then make our plans with **confidence**."

Henry Ford

The year 2008 was a time security threats reached a tipping point, and 2009 stands to be the year critical infrastructure systems become prime targets for fraud and criminals as the global financial crisis will be exploited for a variety of malicious activities. Thus, it is vital for organisations to not only safeguard their infrastructure, but maintain and sustain strong resilience.


marcusevans

Featuring keynote addresses by:

Michael Jerks Assistant Secretary
Critical Infrastructure Protection
National Security Resilience Policy Division
Attorney-General's Department

David I Harris Executive Director
Security & Emergency Management
Department of Transport (VIC)

Attend this premier event and gain insights into:

- The latest development in Critical Infrastructure Protection programme
- Moving towards organisational resilience and ensuring business continuity during a crisis
- Understanding the importance of Public-Private Partnerships to enhance infrastructure security
- Developing an integrated approach that allows organisations to work independently and interdependently to ensure corporate security
- Analysing the impact of financial crisis on business continuity market
- Protecting your organisation's IT infrastructure
- Lessons to be learnt from Victoria's Bushfires

Endorser



***Early Bird & Group Discounts**
Ask about our savings

A tailor-made interactive workshop on:

Securing critical infrastructure against the threat of Climate Change

Facilitated by:

Athol Yates Executive Director
Australian Homeland Security Research Centre

Leading case studies and highly topical presentations by:

Peter Brouggy Banking & Finance IAAG Project Manager
ANZ
Member of the National Resilience Community of Interest

Harry Archer Head of Practice
Business Continuity, Security and Governance Practice
British Telecom

Mike McCluskey State Director NSW
Australian Broadcasting Corporation

Robert Oldfield Managing Director
Organisational Resilience

Tim Janes MBCI Australasian Chapter Committee Member
NSW Chapter Coordinator
Business Continuity Institute (BCI)

Robbie Sinclair Head of Security
Country Energy
Member of the National Resilience Community of Interest

Jeffrey Choi Chief Information Security Officer
Internal Audit and Risk
Coca-Cola Amatil Ltd

Ross Piper Head of Corporate Risk
Macquarie Group

Paul Holman Operations Manager
Specialist Emergency Response Department
Ambulance Victoria

Thursday 11th June 2009

0830 Morning coffee and registration

0850 Welcoming address from the Chair

0900 Session One – Keynote Address

Reviewing the Critical Infrastructure Protection programme: An 'all hazards, all agencies' approach

- Analysing the current security environment and the security challenges facing both business and the Government
- Assessing the impact of First National Security Statement and the New National Counter - Terrorism Alert System on critical infrastructure protection
- Enhancing the relationship between the Federal Government and the private sector – the role of Trusted Information Sharing Network
- Understanding the importance of 'interdependencies' within and between industrial sectors

Michael Jerks Assistant Secretary
Critical Infrastructure Protection
National Security Resilience Policy Division
Attorney-General's Department

0945 Session Two – Case Study

The impact of global financial crisis on business continuity market

The recent survey by Continuity Central show that the majority of organisations expect business continuity spending to hold up in 2009, with 42.5% stating that it would be same in 2009 as it was in 2008 and 20.5% expecting it to be higher. This session will discuss if financial crisis should change the way organisations address business continuity.

- Analysing the meaning of global recession for organisations' Business Continuity Plan
- Underpinning how business continuity management is implemented under normal economic condition
- Assessing the potential hazards which may be intensified by the financial crisis – fraud and supply failure
- Building a cost effective plan while sustaining business value and maintaining security

Tim Janes MBCI Australasian Chapter Committee Member
NSW Chapter Coordinator
Business Continuity Institute (BCI)

1030 Morning refreshments and networking break

1100 Session Three – Case Study

Organisational Resilience - planning for the unpredictable

- Re-defining organisational resilience – an integrated approach of risk management, business continuity management, emergency management and security management
- Analysing the challenges with traditional risk management – how to manage low frequency/high impact risks, those beyond the normal realms or controls
- Identifying the critical elements to build an organisational resilience model – communication, collaboration and coordination
- Enhancing qualities of a resilient organisation
 - Great situation awareness
 - Solid knowledge of keystone vulnerabilities
 - The ability to adapt to a changing situation

Peter Brouggy Banking & Finance IAAG Project Manager
ANZ
Member of the National Resilience Community of Interest

1145 Session Four – Expert Insight

Enhancing the corporate security portfolio and improving your security control framework

- Promoting security awareness among staff thereby achieving a common objective within an organisation
- Aligning security with every business unit to minimise potential risks
- Monitoring the potential security risks on the global, national and regional scales as well as in your industry sector
- Planning for the worst case scenario

Robbie Sinclair Head of Security
Country Energy
Member of the National Resilience Community of Interest

1230 Luncheon

1330 Session Five – Case Study

Applying good organisational leadership practices in a business disruption context

- Understanding the threat context and maintain effective situational awareness
- Partnering with stakeholders to gain their support and tolerance in a disruption event
- Leading with clear direction while empowering problem solving to teams
- Using diverse teams to adapt to disruptions and react flexibly to restore routine functioning and strengthen the organisation
- The influence of organisational culture – investing in the people side of equation

Robert Oldfield Managing Director
Organisational Resilience

1415 Session Six – Case Study

Emergency response and planning: A whole-of-organisation approach

- Preparing and planning – building greater resilience through process, people and practice
- Assessing existing emergency procedures to improve on past performance in a crisis
- Taking a proactive stance and measure the critical time frames for emergency response
- Minimising adverse effects on people, damage to property or harm to the environment in an emergency
- Lessons learnt from Victoria's Bushfires

Paul Holman Operations Manager
Specialist Emergency Response Department
Ambulance Victoria

1500 Afternoon refreshment and networking break

1530 Session Seven – Case Study

Understanding the critical role of media communication in an emergency situation

- The critical role broadcasting, especially plays in times of emergency in our community, such as fire, flood and natural disaster.
- Information flows through radio and online content in emergencies from combat agencies as well as from community to community
- Some case study examples of the critical role played by the ABC in emergencies, what happens when power and other communication modes fail
- The geographic spread of the ABC infrastructure and the essential nature of localism during disasters to provide meaningful information
- The infrastructure requirements essential to the ABC to ensure we maintain local, meaningful content to the audience, e.g. fuel, power, phones, transmission lines, staff access, studios across Australia

Mike McCluskey State Director NSW
Australian Broadcasting Corporation

1615 Session Eight – Case Study

Securing your critical computer systems– the future is cyber security

Critical infrastructure is comprised of all of the computer systems that could be targets of criminal threats, industrial espionage and/or politically motivated sabotage. This session will address the importance of securing critical computer systems to enhance infrastructure security.

- Reviewing the role of Computer Emergency Response Teams (GovCERT.au) and the Computer Network Vulnerability Assessment (CNVA) Programme
- Embracing the rapid changes in the e-security environment and develop an integrated approach to address e-security issues
- The convergence of physical security with e-security
- Evaluating the potential threat of cyber attacks on critical computer networks
- Testing computer networks for vulnerabilities:
 - Software vulnerabilities
 - Authentication and authorization
 - Logging and monitoring
 - Management of network traffic
- Establishing up-to-date security procedures and improving security awareness among staff

Harry Archer Head of Practice (Australia)
Business Continuity, Security and Governance Practice
British Telecom

1700 Closing remarks from the Chair and end of Day One

Who must attend

- Security Managers
- Infrastructure Security Managers
- Risk Managers
- Emergency Service Personnel
- Operations Managers
- Facilities Managers
- Business Continuity Managers
- Business Resilience

From: energy and water supplies, telecommunications, media and communication, healthcare, manufacturing, government, public venues, transport, mineral and resources, supply chain, logistics, iconic buildings and financial institutions

Friday 12th June 2009

0830 Morning coffee and registration

0850 Opening address from the Chair

0900 Session One – Keynote Speech

Working together towards a holistic system resilience

- Highlighting the importance of interdependencies within and between countries and regions for Critical Infrastructure Protection
- Developing awareness of shared resilience despite differences in paradigms and motivations
- Public-private models for collaboration in holistic system resilience
- Lessons to be learnt from Victoria's bushfires - an early view of resilience in adversity
- The importance of creating a true 'champion team not a team of champions'

David I Harris Executive Director
Security & Emergency Management
Department of Transport (VIC)

0945 Session Two – Expert Insight

The human aspect of business resilience and security

- Effective integration of human factors in business continuity and security management
- Identifying human capacity requirements and risks in crisis situations
 - Situational leadership and formal leadership
 - Adaptability
 - Ability to maintain business operations
- Building a culture of resilience
 - The organisational development factor
 - Risk and Vulnerability Assessment
 - Static and dynamic planning

Ross Piper Head of Corporate Risk
Macquarie Group

1030 Morning refreshment & networking break

1100 Session Three – Case Study

Integrating information security into business security strategy and corporate performance measurement

Business security, from an IT perspective, is comprised of enterprise-wide proactively-focused solutions and contingency plans that provide for the right levels of business continuity regardless of circumstances, and allow for quick and efficient recovery in the event of an unplanned interruption of operations.

- Identifying and correcting continuity problems within IT department and achieve greater alignment with corporate security plan
- Lessons learnt from IT outsourcing arrangement (e.g. Warehouse Management System) and the impact to business operation's continuity
- Exploring IT resilience, redundancy and response, not only recover
- Compliance to policing and regulatory requirement vs. operational practicalities

Jeffrey Choi Chief Information Security Officer
Internal Audit and Risk
Coca-Cola Amatil Ltd

1145 Session Four – Panel Discussion

Sharing the successes and challenges of Business Continuity: How is your organisation doing?

- How can Business Continuity Plan be positioned as a leading risk management activity?
- Building the business case for Business Continuity Plan to reduce operating costs, drive revenue and promote community reputation
- Ensuring a cost-effective and sustained organisational resiliency.
- Assessing the trends and best practices in Business Continuity Planning

Panellists:
Robbie Sinclair Head of Security
Country Energy
Member of the National Resilience Community of Interest

Peter Brouggy Banking & Finance IAAG Project Manager
ANZ
Member of the National Resilience Community of Interest

Robert Oldfield Managing Director
Organisational Resilience

1230 Luncheon

1330 Session Five – Expert Insight

Reducing rising fraud and corporate crime – 'An ounce of prevention is worth a pound of cure'

Corporate crime poses a real and substantial threat to the stability of any business. Fraud and theft involving everything from intellectual property to inventory, from cybercrime to corruption, are multi-billion pound problems

- Understanding the existing fraud environment and the 'real' organisational stance toward fraud
- Identifying gaps through fraud management initiatives linked to strategic drivers
- Implementing prevention measures to inhibit a potential leakage
- Allocating accountability and monitoring and reporting progress
- Acknowledging Privacy Act and other legislations relevant to your business

1415 Session Six – Interactive Workshop

Securing critical infrastructure against Climate Change

The global climate is changing, and will continue to change, in ways that affect the planning and day to day operations of businesses, government agencies and other organisations. The manifestations of climate change include higher temperatures, altered rainfall patterns, and more frequent or intense extreme events such as heatwaves, drought, and storms.

The workshop objective is to provide participants with an understanding of the practicalities of developing a Climate Change Adaptation Plan for critical infrastructure. It involves using the Australian Homeland Security Research Centre's analysis methodology to build a structured approach to:

- Identifying relevant climate change variables
- Identifying climate change impacts of relevance on both demand and supply,
- Identifying climate change adaptation options
- Selecting the most cost-effective adaptation measures
- Outlining the key elements in a Climate Change Strategic Adaptation for your organisation

Athol Yates Executive Director
Australian Homeland Security Research Centre

Athol Yates is the Executive Director of the Australian Homeland Security Research Centre (AHSRC) and the AHSRC's Climate Change Infrastructure Adaptation Research Program. His current key project is development of the Climate Change Infrastructure Adaptation Training Course for electrical, railway and emergency services professionals. This is a Department of Climate Change funded project.

His work in climate changes builds on his past research relating to infrastructure vulnerabilities from natural disasters and terrorism. He was formerly the Senior Policy Advisor to Engineers Australia where he was heavily involved in developing Australia's Infrastructure Report Cards.

He is also the author of the 180 page report Engineering a Safer Australia: Protecting Critical Infrastructure and the Built Environment, which is the key public report on Australia's critical infrastructure protection efforts.

Workshop Schedule

1415	Opening and start of workshop
1500	Afternoon Tea
1530	Workshop resumes
1700	Close of workshop and end of Day Two

Why you must attend

Critical infrastructure plays an important role in the social and economic well being of a nation. It is therefore of paramount importance that owners and operators of infrastructure are aware of the ways that they can assess, identify and understand threat and vulnerability to their critical infrastructure as a method for minimising risk.

At any time Australia faces threats from a range of sources which in different ways can put our institutions of state, people, economic assets and technology at risk. The heightened threats of terrorism, human and natural disasters, threats of climate change are indicative of the growing range of threats to infrastructure protection and security in 2008. In 2009 the Australian Government will spend an estimated \$4-4.5 billion in countering, mitigating and responding to these hazards. The safety and security of our critical infrastructure requires the cooperation and input of the business sector, government cannot do it alone.

Following the success of past 3 years, **marcus evans 2009 Critical Infrastructure Protection and Security Forum** will take you further towards the importance of the growing need of organisational resilience and discover the latest development in cooperation and strategic plans from both public and private sectors.

marcus evans would like to thank everyone who has helped with the research and organisation of this event, particularly the speakers and their staff for their support and commitment.

Critical Infrastructure Protection and Security Forum

SY-IF1371 | Please write in BLOCK CAPITALS

Sales Contract

Please complete this form immediately and fax back to

PETER MORGAN

FAX: +61 (2) 9238 7286

Name: _____

Position: _____

Email: _____

Name: _____

Position: _____

Email: _____

Name: _____

Position: _____

Email: _____

Organisation: _____

Address: _____

Town: _____ State: _____ Postcode: _____

Tel: () _____ Fax: () _____

Nature of Business: _____

Company Size: 1-9 10-24 25-49 50-99
 100-249 250-499 500-999 1000+

Authorisation

Signatory must be authorised to sign on behalf of contracting organisation.

Name: _____

Position: _____

Signature: _____ Date: / /

This booking is invalid without a signature.

Fees

- Standard Conference Fee** AUD3,217.80 + GST / VAT (if applicable) per delegate
Conference documentation will be available online. A web site and password will be provided to you before the event.
 - Early Bird 10% Discount*** A limited number of early bird seats are available. Please ask for details.
 - Premier Plus Discount*** Bring 3 or more delegates to this event and benefit from a 10% saving. (Applies to full conference event only).
 - Documentation** @ AUD599 + GST / VAT (if applicable) per set. If you are unable to attend the conference but wish to obtain the conference documentation, please complete the section above and return with payment. A website and password will be provided to access the documentation post-event.
- * These discounts may not be used in conjunction with any other offer.

Business Opportunities

A limited amount of exhibition space is available at the conference. Sponsorship opportunities including lunch and documentation also exist. Please contact **Peter Morgan** on +61 2 9238 7200 or email peterm@marcusevansau.com

Register Now

Contact Peter Morgan at **marcus evans**
T +61 (2) 9238 7200
F +61 (2) 9238 7286
www.marcusevans.com

Code:E

Date: 11th & 12th June 2009
Venue: Swissotel, 68 Market Street, Sydney, NSW 2000, Australia

Hotel Accommodation

Accommodation is not included in the conference fee. To reserve accommodation at the conference venue, please contact the hotel at +61 2 9238 8828 and make it clear that you are attending **marcus evans** conferences event quoting SY-IF1371 as a reference.

marcus evans

Level 5, 99 Bathurst Street, Sydney, NSW 2000, Australia
www.marcusevans.com

Payment Method

Payment is required within 5 working days on receipt of invoice

Credit Card:

Please debit my Visa Mastercard Amex Diners

Card Holder's Name: _____

Card Number:

□□□□ □□□□ □□□□ □□□□

Security Code:

□□□□

Signature: _____ Expiry Date: / /
M Y

Confirmation Details: After receiving payment a receipt will be issued. If you do not receive a letter outlining joining details two weeks prior to the event, please contact the Conference Coordinator at **marcus evans** conferences.

Terms & Conditions:

1. Fees are inclusive of program materials and refreshments.
2. Payment Terms: Following completion and return of the registration form, full payment is required within 5 days from receipt of invoice. PLEASE NOTE: payment must be received prior to the conference date. A receipt will be issued on payment. Due to limited conference space, we advise early registration to avoid disappointment. A 50% cancellation fee will be charged under the terms outlined below. We reserve the right to refuse admission if payment is not received on time.
3. Cancellation/Substitution: Provided the total fee has been paid, substitutions at no extra charge up to 14 days before the event are allowed. Substitutions between 14 days and the date of the event will be allowed subject to an administration fee of equal to 10% of the total fee that is to be transferred. Otherwise all bookings carry a 50% cancellation liability immediately after a signed sales contract has been received by **marcus evans** (as defined above). Cancellations must be received in writing by mail or fax six (6) weeks before the conference is to be held in order to obtain a full credit for any future **marcus evans** conference. Thereafter, the full conference fee is payable and is non-refundable. The service charge is completely non-refundable and non-creditable. Payment terms are five days and payment must be made prior to the start of the conference. Nonpayment or non-attendance does not constitute cancellation. By signing this contract, the client agrees that in case of dispute or cancellation of this contract that **marcus evans** will not be able to mitigate its losses for any less than 50% of the total contract value. If, for any reason, **marcus evans** decides to cancel or postpone this conference, **marcus evans** is not responsible for covering airfare, hotel, or other travel costs incurred by clients. The conference fee will not be refunded, but can be credited to a future conference. Event program content is subject to change without notice.
4. Copyright etc: All intellectual property rights in all materials produced or distributed by **marcus evans** in connection with this event is expressly reserved and any unauthorized duplication, publication or distribution is prohibited.
5. Data Protection: Client confirms that it has requested and consented to **marcus evans** retaining client information on **marcus evans** group companies database to be used by **marcus evans** groups companies and passed to selected third parties, to assist in communicating products and services which may be of interest to the client. If the client wishes to stop receiving such information please inform **marcus evans** local office or email gleavep@marcusevansuk.com. For training and security purposes telephone calls may be recorded.
6. Important note. While every reasonable effort will be made to adhere to the advertised package, **marcus evans** reserves the right to change event dates, sites or location or omit event features, or merge the event with another event, as it deems necessary without penalty and in such situations no refunds, part refunds or alternative offers shall be made. In the event that **marcus evans** permanently cancels the event for any reason whatsoever, (including, but not limited to any force majeure occurrence) and provided that the event is not postponed to a later date nor is merged with another event, the Client shall receive a credit note for the amount that the Client has paid to such permanently cancelled event, valid for up to six months to be used at another **marcus evans** event. No refunds, part refunds or alternative offers shall be made.
7. Governing law: This Agreement shall be governed and construed in accordance with the law of New South Wales and the parties submit to the exclusive jurisdiction of the Courts in Sydney. However, **marcus evans** only is entitled to waive this right and submit to the jurisdiction of the courts in which the Client's office is located.
8. Client hereby acknowledges that he/she specifically authorizes that **marcus evans** charge the credit card listed above for the amount provided herein; that this Contract is valid, binding and enforceable; and that he/she has no basis to claim that any payments required under this Contract at any time are improper, disputed or unauthorized in any way. Client acknowledges that they have read and understood all terms of this contract, including, without limitation, the provisions relating to cancellation.



Air Travel & Accommodation:
FCm Travel Solutions is the corporate division of Flight Centre Limited, one of the world's fastest growing travel innovators and an award winning employer of choice. Please call Flight Centre on 133 133 for all your travel requirements.