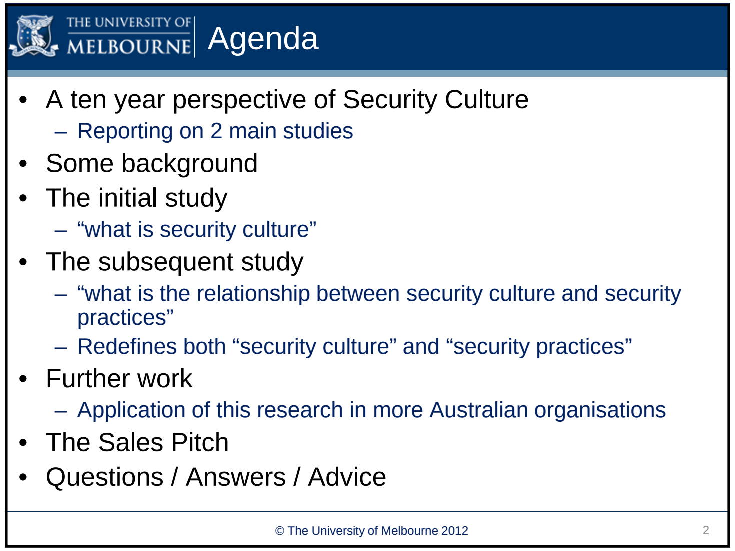
Security Culture

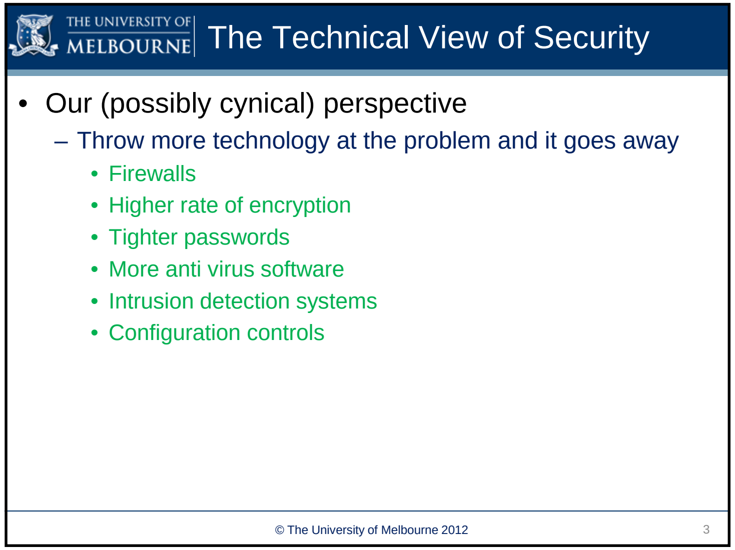
Dr Sean Maynard

Sean.Maynard@unimelb.edu.au
http://people.eng.unimelb.edu.au/seanbm/



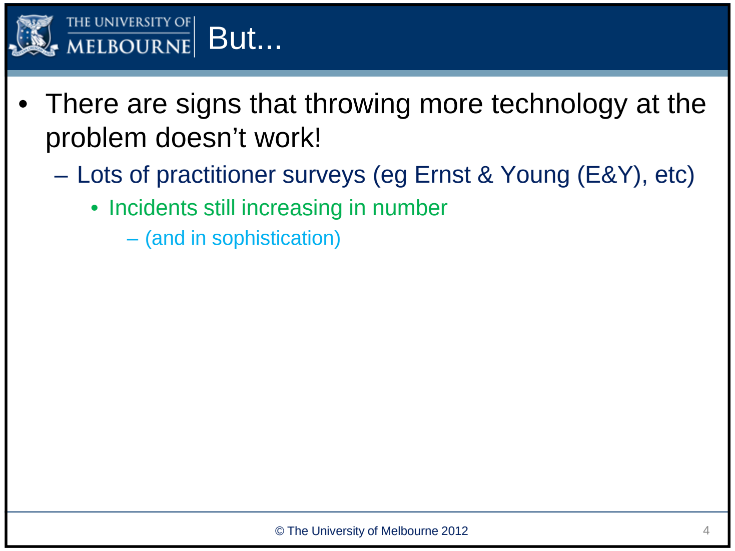
Agenda

- A ten year perspective of Security Culture
  - Reporting on 2 main studies
- Some background
- The initial study
  - “what is security culture”
- The subsequent study
  - “what is the relationship between security culture and security practices”
  - Redefines both “security culture” and “security practices”
- Further work
  - Application of this research in more Australian organisations
- The Sales Pitch
- Questions / Answers / Advice



The Technical View of Security

- Our (possibly cynical) perspective
  - Throw more technology at the problem and it goes away
    - Firewalls
    - Higher rate of encryption
    - Tighter passwords
    - More anti virus software
    - Intrusion detection systems
    - Configuration controls

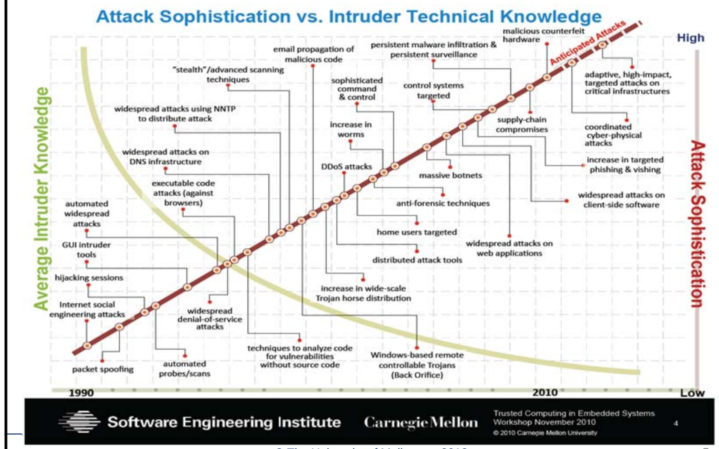


But...

- There are signs that throwing more technology at the problem doesn’t work!
  - Lots of practitioner surveys (eg Ernst & Young (E&Y), etc)
    - Incidents still increasing in number
      - (and in sophistication)

THE UNIVERSITY OF MELBOURNE

But...



THE UNIVERSITY OF MELBOURNE

But...

- There are signs that throwing more technology at the problem doesn't work!
  - Lots of practitioner surveys (eg Ernst & Young (E&Y), etc)
    - Incidents still increasing in number
      - (and in sophistication)
    - Not always from the outside (still)
      - http://www.cert.org/blogs/insider_threat/

THE UNIVERSITY OF MELBOURNE

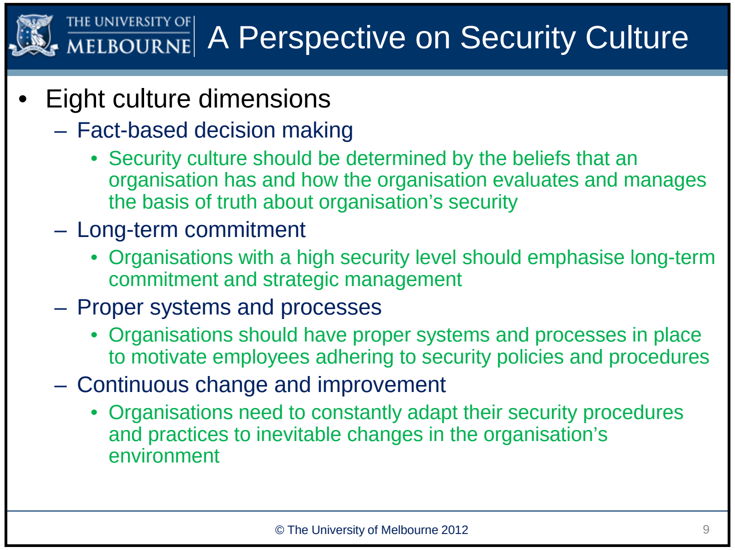
The People Perspective

- Its all about Psychology - How people work
- Differences between generations
  - Baby Boomers
  - Gen X
  - Gen Y
  - Gen Z (Gen Me, Gen Now)
- Culture of the organization
  - Essentially the focus for us should be on...
    - In my organisation do employees see the need for the various security controls and do they actively work towards keeping the organisation secure in their day to day work?

THE UNIVERSITY OF MELBOURNE

The Initial Study

- 2001
  - Lots of data (especially from E&Y, Department of Trade and Industry UK (DTI) showing that >50% of security breaches were from the inside
    - This continues for 5-6 years...
  - Lots of people (researchers and practitioners) were saying that security culture was important if an organisation was to be secure
    - But no one could define what they meant by security culture, or how to measure it...
  - So we attempted to define what security culture was
    - Study was conducted in three organisations
    - Based on a synthesis of concepts from organisation culture

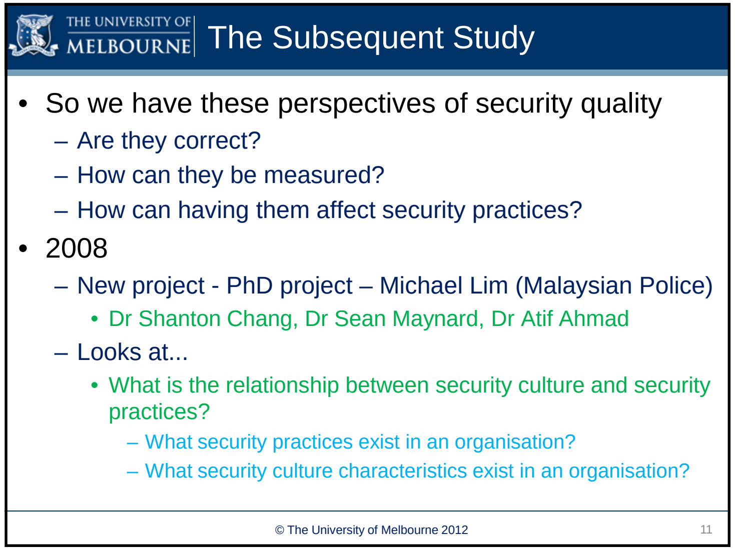


A Perspective on Security Culture

- Eight culture dimensions
  - Fact-based decision making
    - Security culture should be determined by the beliefs that an organisation has and how the organisation evaluates and manages the basis of truth about organisation's security
  - Long-term commitment
    - Organisations with a high security level should emphasise long-term commitment and strategic management
  - Proper systems and processes
    - Organisations should have proper systems and processes in place to motivate employees adhering to security policies and procedures
  - Continuous change and improvement
    - Organisations need to constantly adapt their security procedures and practices to inevitable changes in the organisation's environment

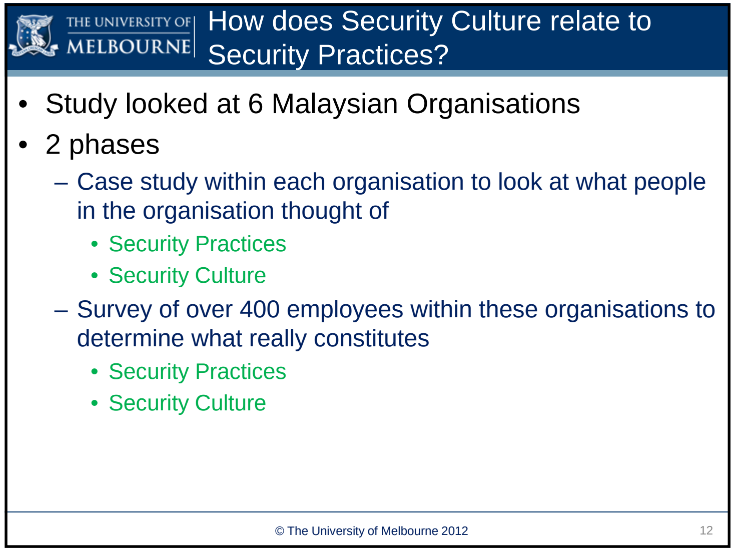
A Perspective on Security Culture

- Eight culture dimensions
  - Employees involvement
    - Employees should be made to feel responsible for security in the organisation by involving them in information security activities and security decision making.
  - Collaboration and cooperation
    - Collaboration and cooperation across organisation is important to improve organisations' security profile
  - A shared vision
    - Members of a high-security culture organisation should hold a shared security visions and goals about organisational security.
  - Internal and external focus
    - Security culture should strike a balance between an internal and external focus.



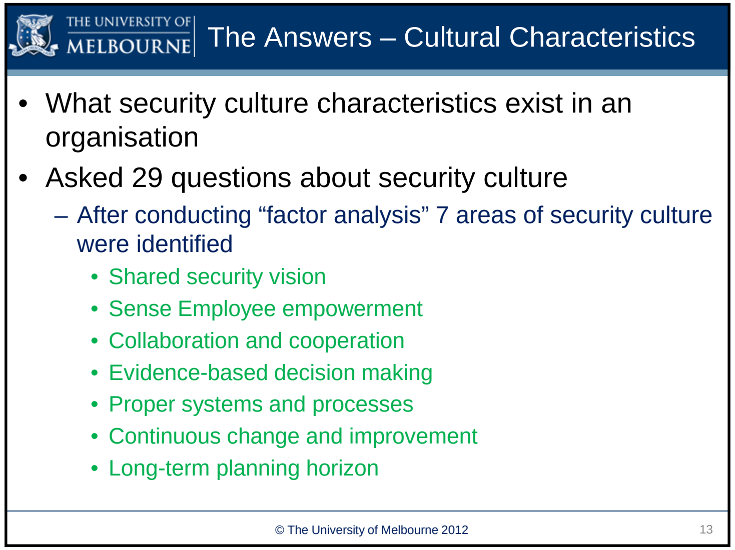
The Subsequent Study

- So we have these perspectives of security quality
  - Are they correct?
  - How can they be measured?
  - How can having them affect security practices?
- 2008
  - New project - PhD project – Michael Lim (Malaysian Police)
    - Dr Shanton Chang, Dr Sean Maynard, Dr Atif Ahmad
  - Looks at...
    - What is the relationship between security culture and security practices?
      - What security practices exist in an organisation?
      - What security culture characteristics exist in an organisation?



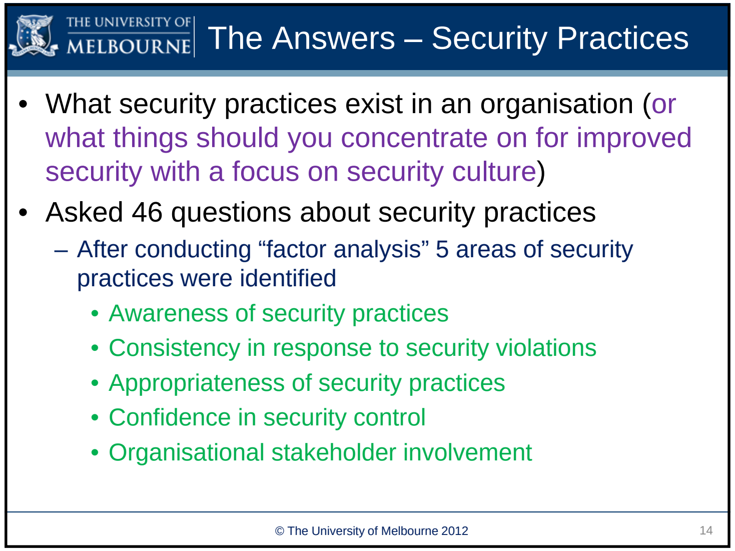
How does Security Culture relate to Security Practices?

- Study looked at 6 Malaysian Organisations
- 2 phases
  - Case study within each organisation to look at what people in the organisation thought of
    - Security Practices
    - Security Culture
  - Survey of over 400 employees within these organisations to determine what really constitutes
    - Security Practices
    - Security Culture



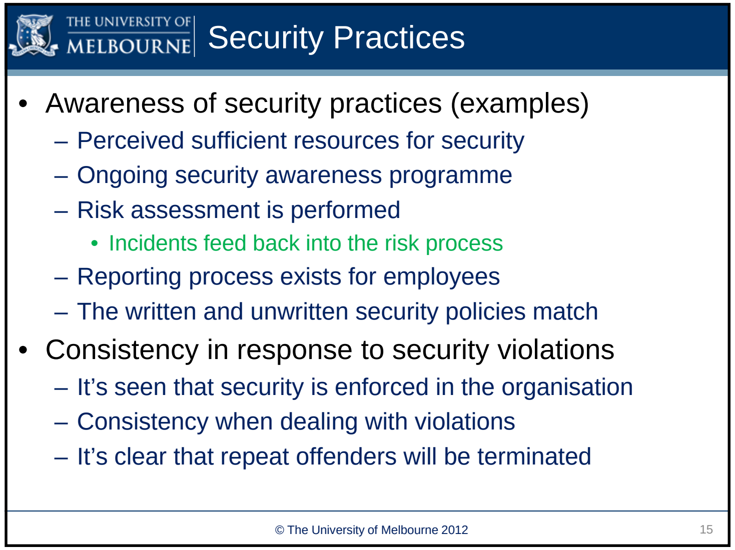
The Answers – Cultural Characteristics

- What security culture characteristics exist in an organisation
- Asked 29 questions about security culture
  - After conducting “factor analysis” 7 areas of security culture were identified
    - Shared security vision
    - Sense Employee empowerment
    - Collaboration and cooperation
    - Evidence-based decision making
    - Proper systems and processes
    - Continuous change and improvement
    - Long-term planning horizon



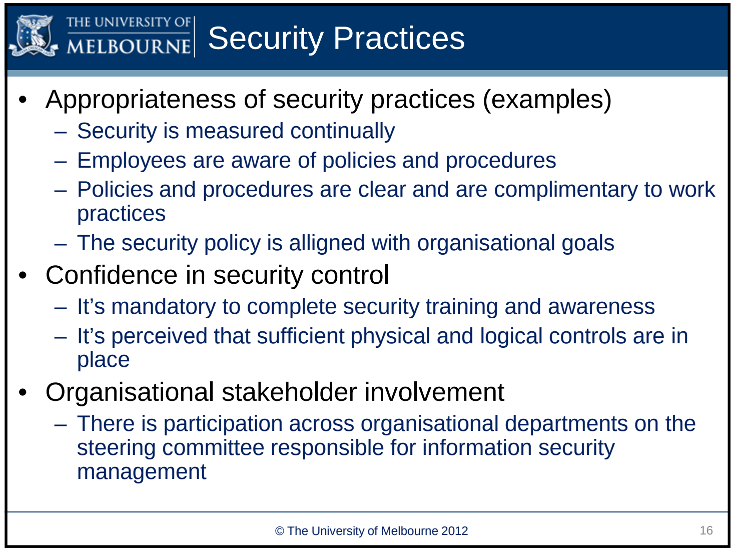
The Answers – Security Practices

- What security practices exist in an organisation (or what things should you concentrate on for improved security with a focus on security culture)
- Asked 46 questions about security practices
  - After conducting “factor analysis” 5 areas of security practices were identified
    - Awareness of security practices
    - Consistency in response to security violations
    - Appropriateness of security practices
    - Confidence in security control
    - Organisational stakeholder involvement



Security Practices

- Awareness of security practices (examples)
  - Perceived sufficient resources for security
  - Ongoing security awareness programme
  - Risk assessment is performed
    - Incidents feed back into the risk process
  - Reporting process exists for employees
  - The written and unwritten security policies match
- Consistency in response to security violations
  - It’s seen that security is enforced in the organisation
  - Consistency when dealing with violations
  - It’s clear that repeat offenders will be terminated



Security Practices

- Appropriateness of security practices (examples)
  - Security is measured continually
  - Employees are aware of policies and procedures
  - Policies and procedures are clear and are complimentary to work practices
  - The security policy is alligned with organisational goals
- Confidence in security control
  - It’s mandatory to complete security training and awareness
  - It’s perceived that sufficient physical and logical controls are in place
- Organisational stakeholder involvement
  - There is participation across organisational departments on the steering committee responsible for information security management

The Answers – Relationships

- Positive and significant relationship between
  - Shared security vision and security practices
    - Top down push of security vision to employees
      - In such a way to get employees to align their actions to this vision
    - Set KPI's to enable security
    - The power of coordinated action to achieve security
  - Employee empowerment and security practices
    - Give employees responsibility around security
      - Foster a sense of ownership
    - Clear set of expectations to improve security
      - Good "reporting" mechanisms
      - Feel obliged to help

The Answers – Relationships

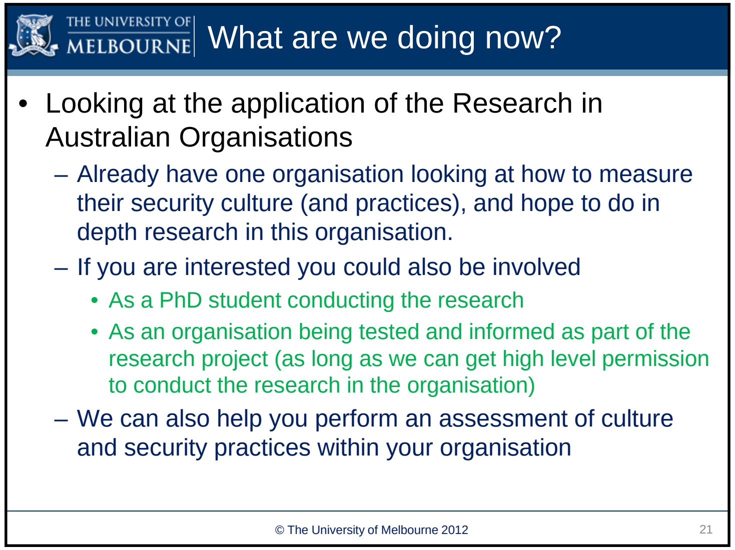
- Positive and significant relationship between
  - Collaboration and cooperation and security practices
    - Important that security is a whole of organisation initiative (not just a small group)
      - To ensure effective security
      - To ensure security completeness and recognition
      - Shows employees that it's serious
  - Evidence-based decision making and security practices
    - Base security decisions / actions on evidence
      - eg - gauge security awareness on DATA!
      - Use KPI's set up to gauge employees' willingness to engage with security
      - Are your security actions successful??
        - » If you cant measure it how do you know it works

The Answers – Relationships

- Positive and significant relationship between
  - Proper systems and processes and security practices
    - Ensure that systems and processes are visible to employees
      - Employees motivated to adhere
        - » Be careful of different generations...
- No significant relationship between
  - Continuous change & improvement and security practices
    - Focus on stability of policy and processes whilst having the capacity for change as required...(eg handling a new threat)
  - Long-term planning and security practices
    - Planning horizon has no impact on security practices
      - Lots of it is "fire fighting" and perception management

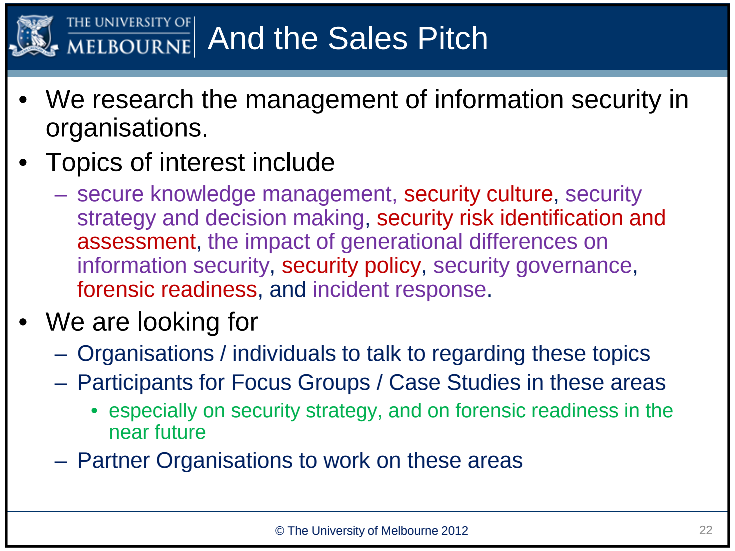
Some Issues

- The study was conducted in Malaysia
  - There are inherent cultural biases involved
- Study had limited scope
  - Only 6 organisations (although a large number of participants - 453)
    - Can't tell if we can reliably predict what would happen in other organisations
      - Although if you are in Malaysia in one of the targeted industries we are confident



What are we doing now?

- Looking at the application of the Research in Australian Organisations
  - Already have one organisation looking at how to measure their security culture (and practices), and hope to do in depth research in this organisation.
  - If you are interested you could also be involved
    - As a PhD student conducting the research
    - As an organisation being tested and informed as part of the research project (as long as we can get high level permission to conduct the research in the organisation)
  - We can also help you perform an assessment of culture and security practices within your organisation



And the Sales Pitch

- We research the management of information security in organisations.
- Topics of interest include
  - secure knowledge management, security culture, security strategy and decision making, security risk identification and assessment, the impact of generational differences on information security, security policy, security governance, forensic readiness, and incident response.
- We are looking for
  - Organisations / individuals to talk to regarding these topics
  - Participants for Focus Groups / Case Studies in these areas
    - especially on security strategy, and on forensic readiness in the near future
  - Partner Organisations to work on these areas

Questions / Comments / Advice

Contact Details

Sean.Maynard@unimelb.edu.au

http://people.eng.unimelb.edu.au/seanbm/

Thank You

THE UNIVERSITY OF MELBOURNE