

# Readiness, Response and Recovery



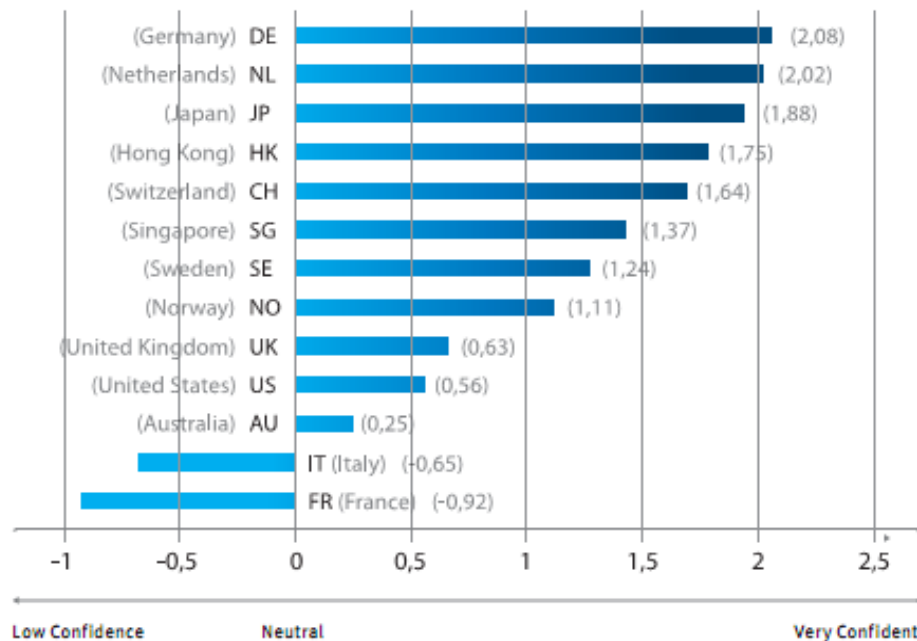
David Tattam  
Director

# Agenda

1. Readiness – David Tattam
2. Case Studies on Response and Recovery:
  - Bill Armagnacq (Heritage BS)
  - Royden Juriansz (CUA)
  - Lewis von Stieglitz (Warwick CU)

# Readiness Survey

Chart: Acronis Global Disaster Recovery Index 2011



3048 respondents – 259 from Australia

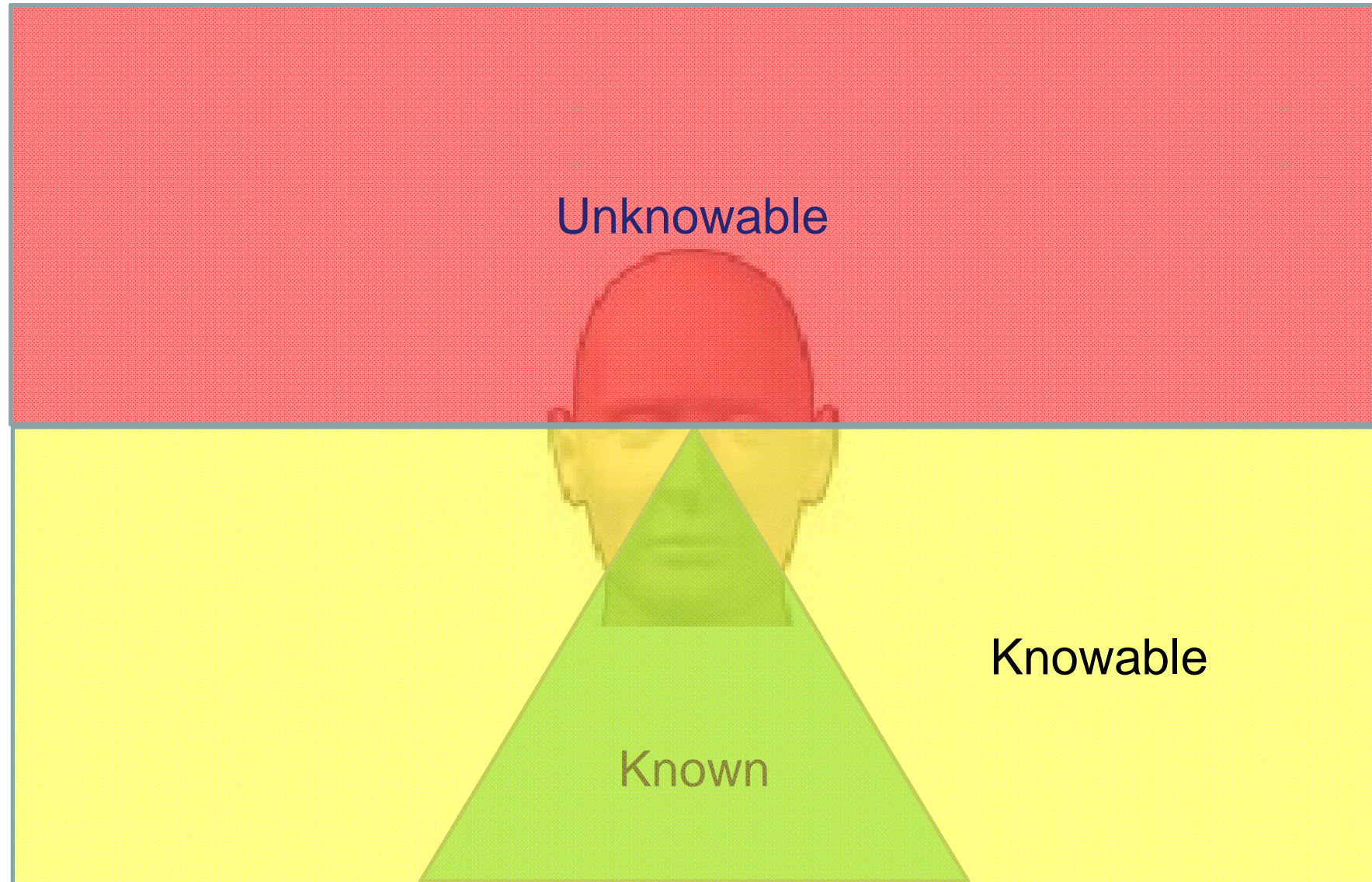
## Australia. Poor in:

- Ability to avoid downtime in the event of a serious incident 44%.
- Confidence in recovering quickly 36% - Germany (77%)
- Low boardroom buy-in
- Lowest confidence in successfully recovering from a serious incident. 22% (global average - 50%).
- Third of businesses in Australia (36%) do not have an offsite backup and DR strategy in place. Australia spent consistently less on backup and DR 11% than Germany (13%).

# Ready for What?

- The obvious ones
  - Acts of nature: Weather, Seismic, Solar, Bushfire, Flood
  - Acts of people: Terrorism, War, Civil unrest, Kidnap, Siege
  - Health: Pandemic, Poisoning, isolated outbreak
  - Accidents: Fire, collapse, hazard spill, communications cut
- What is reasonable? “Extreme but Plausible”
- The less obvious ones
  - Loss of key staff
  - Equipment failure
  - Reputation damage
- Any event that can cause material business disruption

# Risk Awareness



# Ready?

“To make ready beforehand for a specific purpose, as for an event or occasion”

- Set
- Organised
- Equipped
- Geared up
- Arranged
- Primed
- Confident you will cope

# The event is a crisis !



- You will never be perfectly ready
- You will be in stress
- You will resort to embedded response
- You will want to modify your plans
- You will need to problem solve on the fly

**You need to be PRACTICED**

# Phases to be ready for

1. How will you immediately respond?
2. How will you limit damage?:
  - Infrastructure
  - Information
  - Staff / people
  - Processes
3. How will you recover? How well and how quick?
4. How will you ensure business continues?

## 2. Guidance and Standards

- APS 232 (CPS 232): Risk Assessment and Business Continuity Management
- ISO 31000: Risk Management: Principles and Guidelines

# CPS 232

A regulated institution's BCM must, at a minimum, include:

- (a) a BCM Policy;
- (b) a business impact analysis (**BIA**) including risk assessment;
- (c) recovery objectives and strategies;
- (d) a business continuity plan (**BCP**) including crisis management and recovery; and
- (e) programs for:
  - (i) review and testing of the BCP; and
  - (ii) training and awareness of staff in relation to BCM.

# Steps

- **BCM:** ensure critical business functions can be maintained, or restored in a timely fashion.
- **Critical Functions:** functions, resources and infrastructure which if disrupted has the potential to impact materially on the ADI's business operations, reputation or profitability. Don't forget critical people!
- **Risk Assessment:** Plausible disruption scenarios
- **BIA:** Impact of losing critical functions
- **Recovery:** Strategies including insurance
- **BCP:** Procedures, Resources, Communications
- **CMP:** Plan for immediate response
- Integrated with the overall risk management process

# The Risk Management Process

1. Communication and consultation
2. Establishing the context
3. Risk identification
4. Risk analysis
5. Risk evaluation
6. Risk treatment
7. Monitoring and review



Licensed to Mr David Tatlam on 16 December 2009. 1 use only. Personal use only. Standards Australia. All rights reserved. (1007683).

## 3. Risk Assessment and BIA

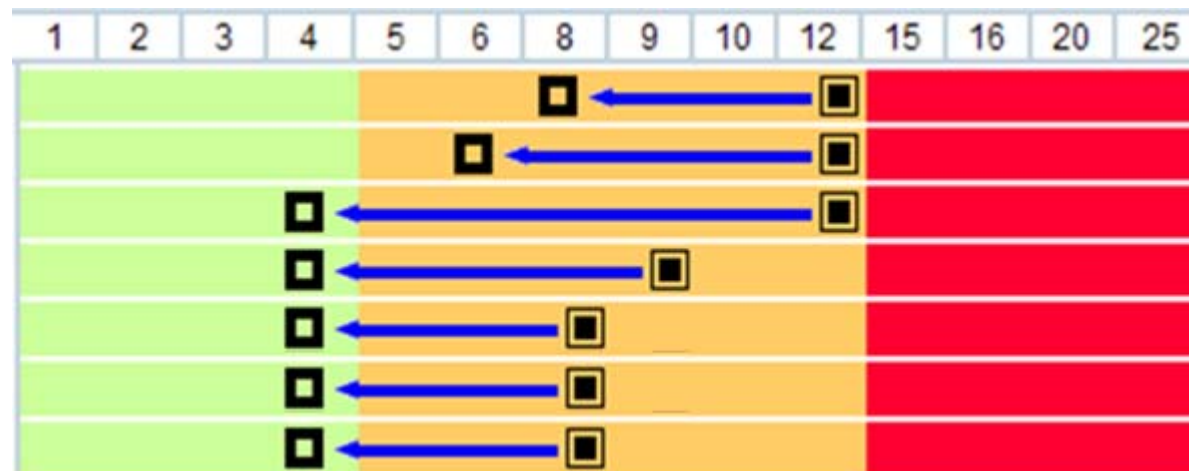
- Identify plausible scenarios and assess likelihood
- Identify critical processes, resources and functions
  - Know your processes
  - What do they impact?
  - What are the single points of failure?
  - Remember human resources – key person, key team
  - IT resources (in source, outsource), Non IT resources, Human
  - Data and information
- BIA
  - How long will critical processes be lost? / Recovery Time Objective (RTO)
  - What impact will loss have?
  - How big will impact be?

# BIA Risk Assessment

Inherent Risk  
 Residual Risk

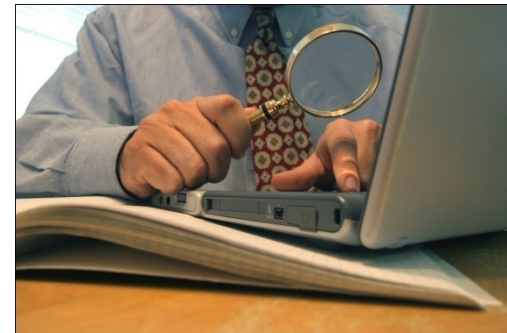
## Loss of

- Access to Premises
- Access to core systems
- Access to Internet
- Access to records
- Access to data
- Loss of landline telecoms
- Loss of mobile telecoms



## 4. Controls and Plans

- **Preventive** – prevent the interruption / limit the interruption (e.g. Sprinklers, Comms room on lvl 20, diversify geographically)
- **Detective** – Detects the impending interruption (e.g. smoke detectors, media monitoring etc).
- **Reactive** – Response and recovery (e.g. Insurance, DRP / BCP / Contingency / Crisis plans)



# The Plans

- Time to recover vs. cost
- Need problem solvers – always something from left field. Do you have people you can rely on in a crisis?
- Use technology – cloud ware, virtualisation, smart devices
- Staff – how to communicate, where will they go, welfare, how will they do their job, how will they react in crisis?
- Understand and manage partnerships. Police, Fire, Builders, IT Consultants, Other Mutuals etc. How long will they take to react?
- Coordinated actions – not piece meal
- Making the plans real and workable
  - Testing. Make them real as possible to get emotional response – see how they react.
  - Training
  - Watch out for the small things
    - Accessible information (Staff action plans, critical info)
    - Human reactions in a crisis

# Insurance as a reactive control

- Is it adequate? Coverage of events, sufficient value?
- Do you know what is covered and what is not? Problems where interruption does not occur at your site. Flood damage often not covered.
- Is your coverage and excess levels commensurate with your risk appetite?
- How quick will pay-outs occur?
- Floods cost industry \$20bn – most expensive natural disaster in Australia’s history. Insurance cost increasing (+10% to + 20%). *“If you demonstrate that you have quality risk management procedures in place, show that you’re taking all reasonable steps to minimise risk and are transparent about how you run your business, you will always be in the best position to get a good price”* Paul Venning: National General Manager for Corporate – Aon Risk Services

# Testing

1. Desktop Review / Senior Staff Review
2. Desktop Scenario Test
3. Interdepartmental Review
4. Notification and call-out communications test
5. Component Testing
6. Business Recovery Test

## 5. Monitoring Readiness

Require a process to ensure constant adequate state of readiness – How?

1. Monitor Key Control Indicators
2. Carry out ongoing control compliance attestations
3. Carry out regular testing
4. Ensure all staff, including new / moved staff are trained
5. Regular update of the risk assessment, BIA and plans

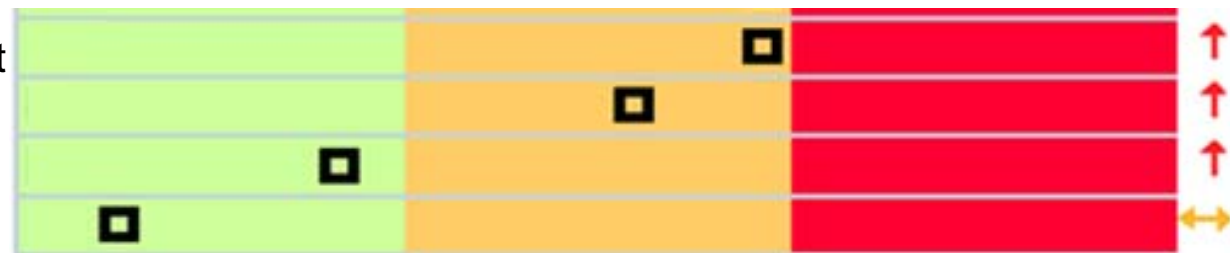
# Monitor

- Key Risk (Control) Indicators
  - Number of months since last BCP test
  - Number of months since fire extinguishers last checked
  - BCP test score
  
- Compliance
  - External – confirm compliance with APS 232
  - Internal
    - Confirm that you have backed up data
    - Confirm that you have carried out BCP test
    - Confirm that you have attended DRP training

# Key Control Indicators

## Key Control Indicator



















1. Months since last BCP test
2. Months since last fire test
3. % of staff trained in BCP
4. Last BCP test result



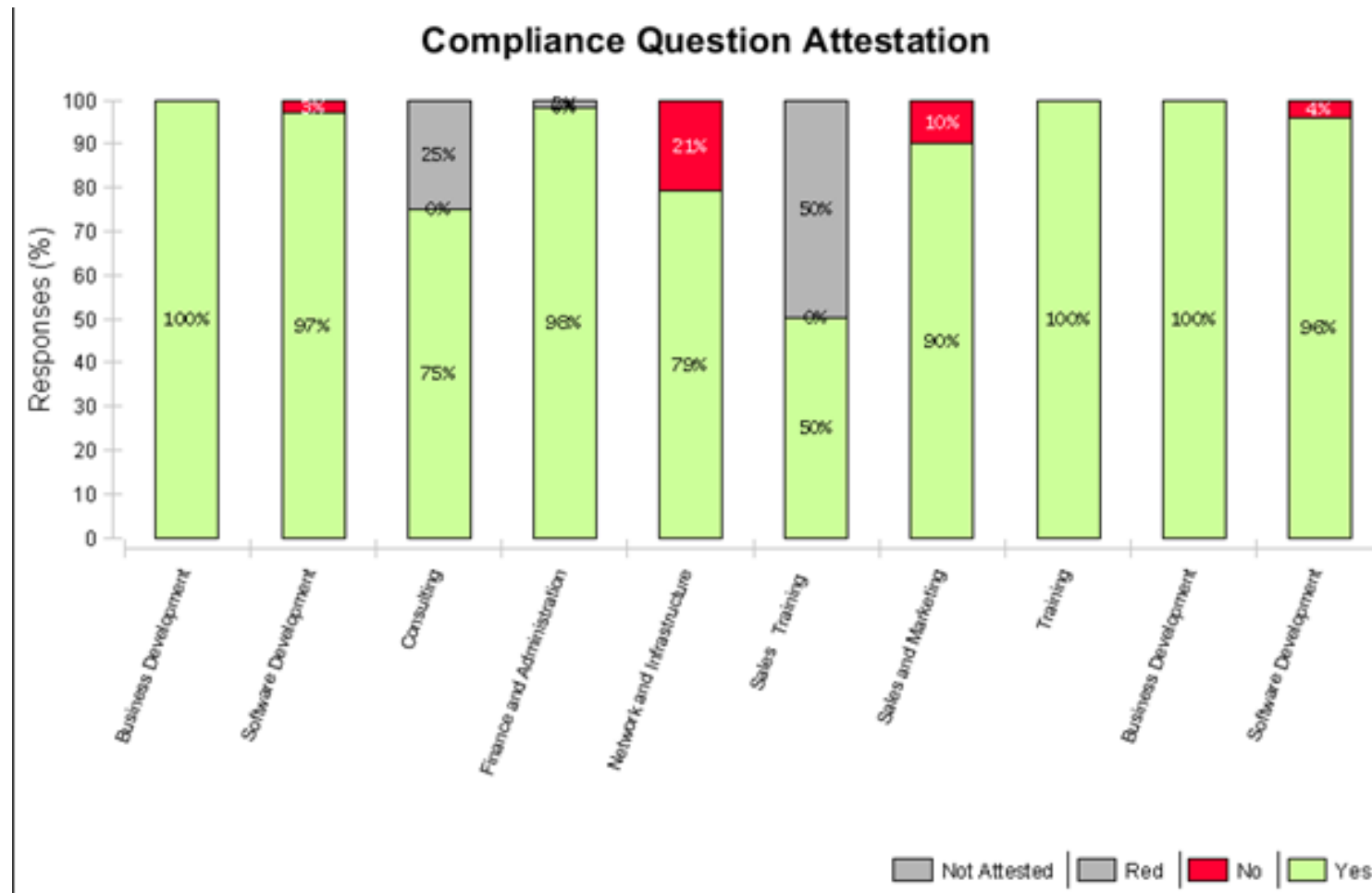
# Compliance

System Client Setup Self Assessment Compliance Key Risk Indicators Incidents Actions WorkFlow Reporting Library

Field: All Fields Filter:

Name
<ul style="list-style-type: none"> <li>▲  APS 232 Business Continuity Management           <ul style="list-style-type: none"> <li>▶  A. Authority and application</li> <li>▶  B. Business continuity management</li> <li>▶  D. Critical business functions, resources and infrastructure</li> <li>▲  E. Risk assessment               <ul style="list-style-type: none"> <li> 14. Please confirm that you have identified plausible disruption scenarios that may lead to short, medium and long-term disruptions to critical business functions and assess the likelihood of these scenarios occurring?</li> </ul> </li> <li>▲  G. Recovery strategy               <ul style="list-style-type: none"> <li> 23. Please confirm if there are insurance arrangements in place to cover some of the costs of business disruption? Please add in the comment field details of insurance coverage.</li> <li> 21. Please confirm that based on the Business Impact Analysis you have considered appropriate recovery strategies?</li> <li> 22. Please confirm that Senior management have approved the resources needed to implement the agreed strategy and have ensured sufficient budgetary and other resources are allocated to allow implementation of t</li> </ul> </li> <li>▲  C. The role of the Board and senior management               <ul style="list-style-type: none"> <li> 11. Info Only</li> <li> 10. Please confirm that Senior management have established clear lines of accountability and reporting for individuals with BCM responsibility?</li> <li> 09. Info Only</li> <li> 08. Please confirm that the Board of Directors, or in the case of a foreign branch, the senior officer outside Australia with delegated authority from the Board, is ultimately responsible for the business continuity of the A</li> </ul> </li> <li>▲  F. Business impact analysis               <ul style="list-style-type: none"> <li> 15. Please confirm a business impact analysis identifying all critical business functions, resources and infrastructure and assessing the impact of a disruption on these has been completed?</li> <li> 17. (a) Please confirm that you have considered the following when determining the potential financial, legal, reputational and other material consequences if the critical business functions, resources and infrastructure</li> </ul> </li> </ul> </li> </ul>

# Compliance



# Readiness, Response and Recovery

## Thank You



David Tattam

Director

[david.tattam@protecht.com.au](mailto:david.tattam@protecht.com.au)