Critical Infrastructure Laws in Australia

Dr Bruce Tonkin, Chief Operating Officer, .au Domain Administration Limited (auDA)

ccTLD News Session #2 – Thursday, 1 October 2020
# Australian Cybersecurity strategy

**Vision:**
A more secure online world for Australians, their business and the essential services upon which we all depend

<table>
<thead>
<tr>
<th>Actions by governments</th>
<th>Actions by business</th>
<th>Actions by the community</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Themes:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Protect critical infrastructure, essential services and households</td>
<td>• Improve baseline security for critical infrastructure</td>
<td>• Access and apply guidance and information on cyber security</td>
</tr>
<tr>
<td>• Combat cyber crime, including on the dark web</td>
<td>• Uplift the cyber security of SMEs</td>
<td>• Make informed purchasing decisions</td>
</tr>
<tr>
<td>• Protect Government data and networks</td>
<td>• Provide secure products and services</td>
<td>• Make informed purchasing decisions</td>
</tr>
<tr>
<td>• Share threat information</td>
<td>• Grow a skilled workforce</td>
<td>• Report Cyber crime</td>
</tr>
<tr>
<td>• Strengthen cyber security partnerships</td>
<td>• Take steps to block malicious activity at scale</td>
<td>• Access help and support when needed</td>
</tr>
<tr>
<td>• Support business to meet cyber security standards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Enhance cyber security capabilities</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Critical infrastructure definition

• Australia’s Government’s Critical Infrastructure Resilience Strategy currently defines critical infrastructure as:

  ‘those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic wellbeing of the nation, or affect Australia’s ability to conduct national defence and ensure national security.’

• For further information see: https://cicentre.gov.au/

- Currently covers critical assets in:
  - Electricity
  - Port
  - Water
  - Gas
  - An ability for the Government to declare an asset as critical

- 2020 discussion paper, is proposing to include:
  - Banking and finance
  - Communications
  - Data and the Cloud
  - Defence Industry
  - Education, research and innovation
  - Energy
  - Food and grocery
  - Health
  - Space
  - Transport
Classes of critical infrastructure entities

- Systems of National Significance
- Regulated Critical Infrastructure Entities (e.g. telcos)
- Critical Infrastructure Entities
In considering whether an asset is of national significance, the Government will consider:

• **Interdependency with other functions**
  - including: the potential for a domino effect if the function were compromised; and vulnerabilities within and between systems and networks.

• **The consequence of compromise to the entity**
  - including: immediate threat to life; sensitivity of data; and broader impacts on economy, security, sovereignty and the well-being of Australians.
Positive Security Obligations

For regulated critical infrastructure entities:

**Principles-based outcomes**
1. Identify and understand risks ✅
2. Mitigate risks to prevent incidents ✅
3. Minimise the impact of realised incidents ✅
4. Effective Governance ✅

**Security Obligations**
- Physical security ✅
- Cyber security ✅
- Personnel security ✅
- Supply chain security ✅
Enhanced Cyber Security Obligations

• For Systems of National Significance

• Situational awareness ✔
• Participation in preparatory activities
  • Cyber security activities ✔
  • Playbook ✔
## Government “direct action”

### Enhanced situational awareness

<table>
<thead>
<tr>
<th>In most circumstances</th>
<th>Where there is an imminent or realised threat, Government may direct protective action and collaboration</th>
<th>In a declared emergency: Government can assist industry to protect critical infrastructure and mitigate the impact of a cyber attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industry will detect and act on threats</td>
<td>Imminent/realised threat detected</td>
<td>Declared Emergency</td>
</tr>
<tr>
<td>↓</td>
<td>➔</td>
<td>➔</td>
</tr>
<tr>
<td>↓</td>
<td>➔</td>
<td>➔</td>
</tr>
<tr>
<td>➔</td>
<td>➔</td>
<td>➔</td>
</tr>
<tr>
<td>Government direction</td>
<td>Entity takes action</td>
<td>Government takes action</td>
</tr>
<tr>
<td>Entity takes action</td>
<td>Entity takes action</td>
<td></td>
</tr>
</tbody>
</table>

### Source: