Media and Cybersecurity

Understanding Upstream and Downstream Dependencies

Cyber and media

Cyber threat continues to grow

Increasing cyber attacks from more players

- state sponsored snooping and influence
- phishing and identity fraud
- denial of service attacks
- malware & ransomware
- malicious insiders

Media
a high profile target

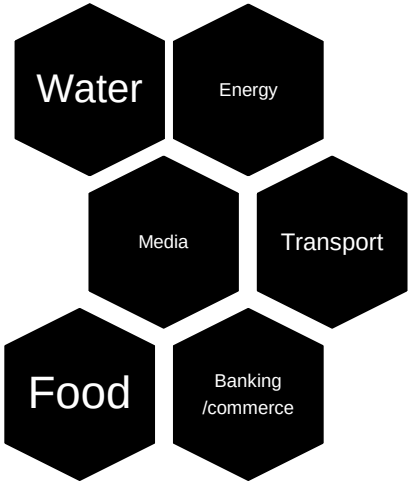
- Media attracts attention from all types
- internationally and locally recognised brands
- occasional controversial statements made on air
- objection to talent or programming from activist groups

- Broadcasters have loyal listeners and lots of valuable information about them

Attracts hackers, snoopers and those who gain satisfaction from attempting denial of service on media sites

Where does media fit in big picture of critical infrastructure?

Media & Communications



Public communication

- Public health - safe drinking water, water shortage, flood alerts
- Energy – blackouts, disruption to supply, refinery issue, fuel shortage
- Public transport, roads, freight, air
- Banking, transactions
- Food safety and supply
- General information, analysis, advice
- Community engagement

Building resilience - partnerships

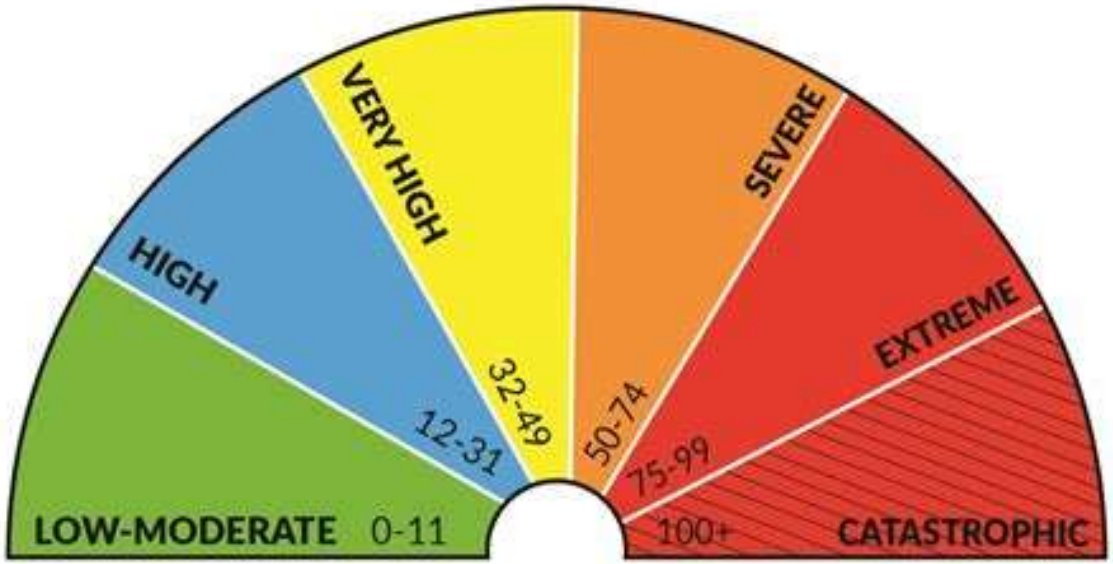
Government

- Threat intelligence & reporting
- Response management
- International collaboration
- Training and Awareness
- Exercises and modelling
- Coordination across agencies

Industry

- Securing information & assets
- Resilient networks
- Constant vigilance
- Testing back up
- Staff training
- Cross sector collaboration & modelling

Continually assess the risk



Media response

- Top down approach – Management need to understand the risk and support actions to defend the organisation
- Sophisticated targeted attacks, so media need more sophisticated responses – machine learning can help anticipate and counter sophisticated attacks.
  - May need to outsource e-security to specialists
- Secondary attacks can be made on advertising partners & less protected associates to try back door access.
- Report cybercrime – i.e ACORN Australian Cybercrime Online Reporting Network

Broadcasting is critical infrastructure

Understand your upstream vulnerabilities

- Risks to studios & equipment
  - Power supply
  - Building access – structural integrity and safety
  - Equipment is compromised

  Solutions: Options for production hubs and remote access, offsite production studio
- Key employees
  - Health & safety of them and their families
  - Ability to travel to work or gain remote access
  - Fatigue
  - OH&S consideration of the workplace – i.e. access via lifts, power for lighting, food, water for toilets,

Broadcasting is critical infrastructure

Understand your upstream vulnerabilities

- Contribution network
    - Telco exchange building affected, fibre/access cable cut
    - Wireless links (i.e studio – Tx microwave link is maliciously overloaded, physical damage
    - Satellite - weather disruption – cyclones
    - Cellular – jammers, local base station disruption

Solutions:

– Options for redundant equipment or paths, NEW dedicated mobile capacity
– Change passwords on routers regularly – don't leave on default password (Admin@supplier name)

Broadcasting is critical infrastructure

Understand your downstream vulnerabilities

- Transmission site

  - Tower and antenna damage
    - fires, cyclone damage, physical attack, extended power outage, fuel shortage, no site access

  - Transmitter Building
    - access – structural integrity and safety
    - Equipment damage or compromise

  - Understand and communicate the extent of the service area and population of impact – may be greater if the site feeds daughter sites

  Solutions: Options for redundant equipment or sites, shared infrastructure, borrowed spares and technical effort, use Defence to assist restorations

Media must be ready

Tips for media outlets

Credits: Australian Cyber Security Centre

Cyber resilience

Protecting your networks and information

- Update anti virus protection for files and emails
- Latest firmware and software updates – patch software vulnerabilities frequently
- Firewalls – restrict the ports to reduce access to network remotely
- Regular password changes – users, admin
- Daily back up – in cloud, hard drives with off site storage
- Employees education/training – awareness/notifications of threats

Cloud infrastructure

- Know your data centre security – where information held, what laws govern it, who has access, do they have back up power
- Security – when do they off shore – do they advise?
- Back up on websites – either do it in house or check it is done if you have a managed service.

- Phones system security
- Cyber insurance
- Building and hardware security

CRITIAL RESPONSE EXERCISE

Build scenarios to test your plan

Exercise planning

- Cyber attack is not our only focus
- All hazards
  - Environmental/climate events
  - Health (pandemic, seasonal)
  - Energy, Water, Transport disruptions
  - External/Global event

…or a combination of several events simultaneously

Scenario building

Ship full of sick passengers arrives in Townsville while they are recovering from a major flood

Passengers - multiple languages, isolation areas already in use

Use emergency and added features available on DAB+ and hybrid to provide

- safety messages and response
- provide easy access for community to report local knowledge on your social assets
- help target where volunteer effort is required

Thank you and good luck!