TECHLAW AUSTRALIA

Update on cyber security and data protection

Thursday, 22 June 2017

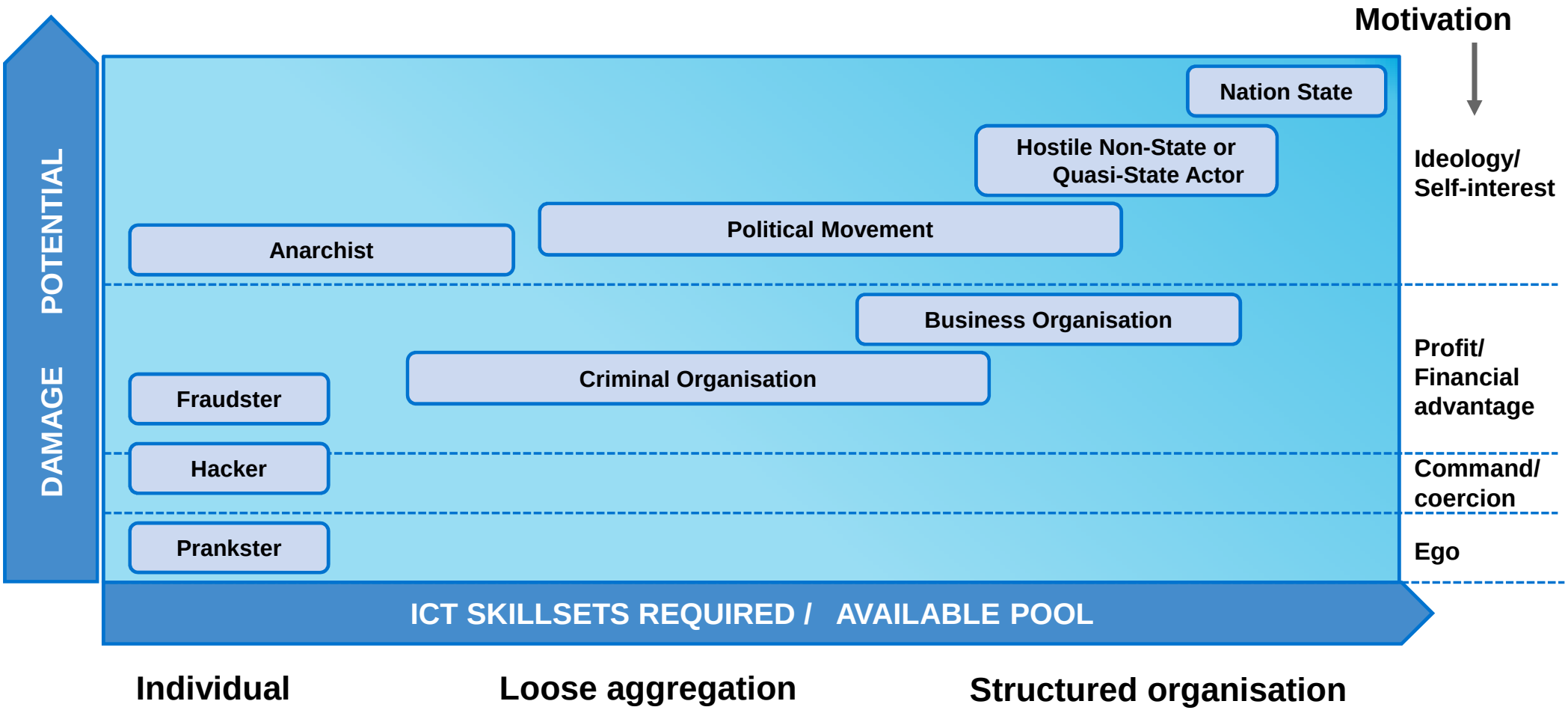
Overview

- Current threat environment – why now?
- What is required/expected?
- Scenarios: Response?

Current Threat Environment - Strategic Importance

- Diverse and evolving legal and regulatory landscape
- Exponential growth of information
- Growing protection challenge
- Corporate requirements and privacy collide
- Data and information breaches/disputes - High cost of mistakes

Not all actors are equal



Some specific statistics from Australia

Australian Cyber Security Centre Threat Report 2016

- Public Sector (18 months to 30 June 2016) : 1095 serious attacks
  - Australian Bureau of Statistics DDOS attack
- Private Sector (18 months to 30 June 2016) : CERT (responding to major incident) responded to 14,804 attacks, 418 of which related to critical infrastructure or systems of national interest

Mandatory Data Breach Notification

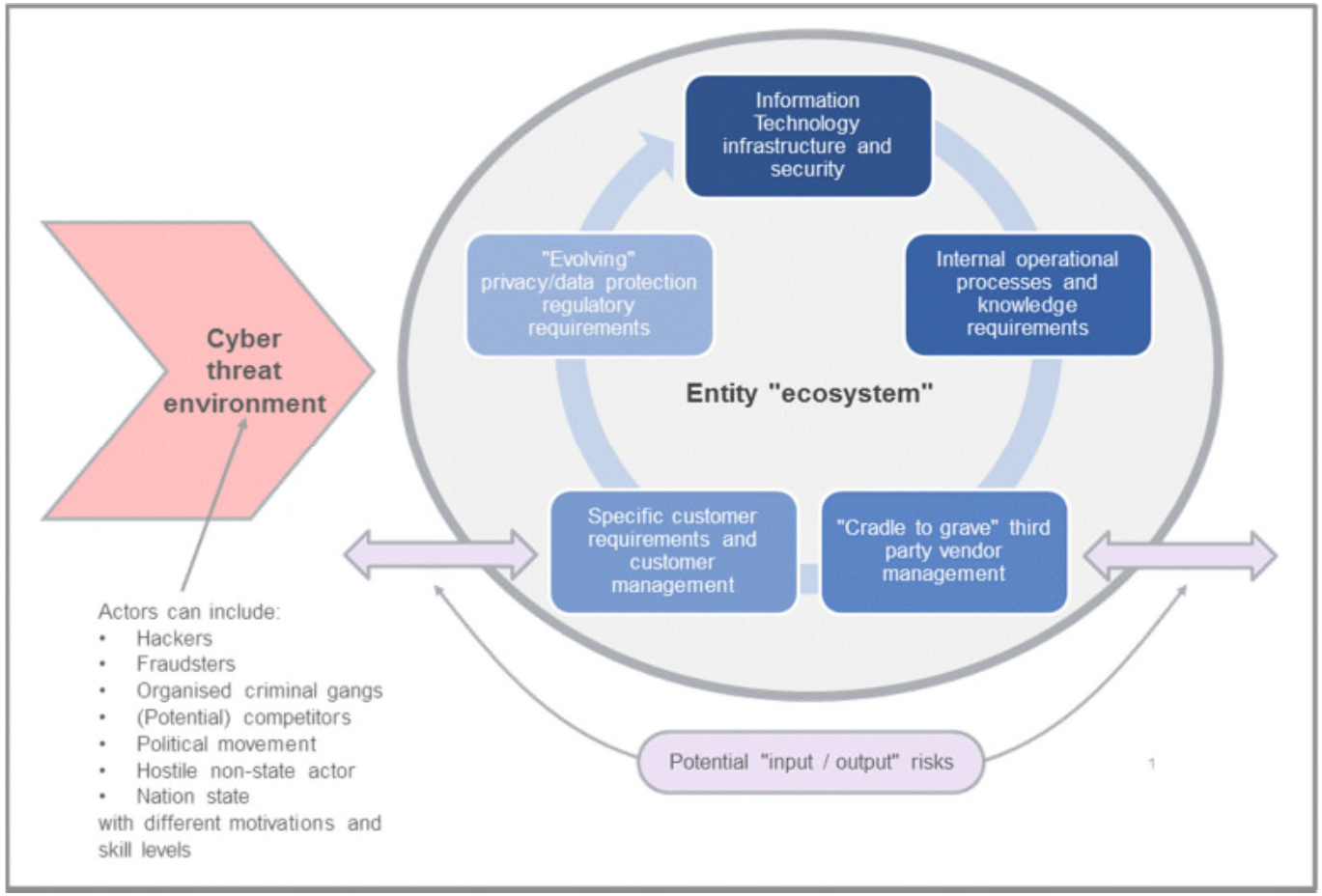
- *Privacy Amendment (Notifiable Data Breaches) Act 2016*
- Due to commence 22 February 2018 (or earlier)
- Notification obligations apply if:
  - the entity becomes aware that there are reasonable grounds to believe that there has been an eligible data breach; or
  - the Information Commissioner so directs the entity.
- 'Eligible data breach':
  - unauthorised access to, or unauthorised disclosure of, or loss of personal, credit reporting or credit eligibility information or TFN;
  - a reasonable person would conclude that the access or disclosure would be likely to result in **serious harm** to an individual to whom the information relates.
- Obligation to assess 'suspected' data breaches
- And then there is the actual notification itself…

ASIC guidance and requirements

- **Report 429 - "Cyber resilience: Health check" – published in March 2015**
- ASIC noted that corporates must consider how and when a cyber attack may need to be disclosed as market-sensitive information in accordance with continuous disclosure obligations
- Directors' obligations to take cyber risks into account when discharging their duties in considering risk management issues
- We are seeing more active engagement of the board and senior executives in data management issues

Core functions and factors involved in a cyber-resilience framework

An integrated view of cyber-risk management?



A response timeline

- Who is on the Incident Response Team (internal / external)?
- [Tested] Incident Response Plan in place
- Proactive penetration testing / vulnerability assessments

- Implement Incident Response Plan, e.g.
  - mobilise IRT
  - segmented, secure communications in place
  - maximise availability of legal professional privilege
- cyber insurance notification? *NB Future actions may be informed by insurance arrangements / requirements*

A response timeline cont.

Contain the breach / preliminary assessment

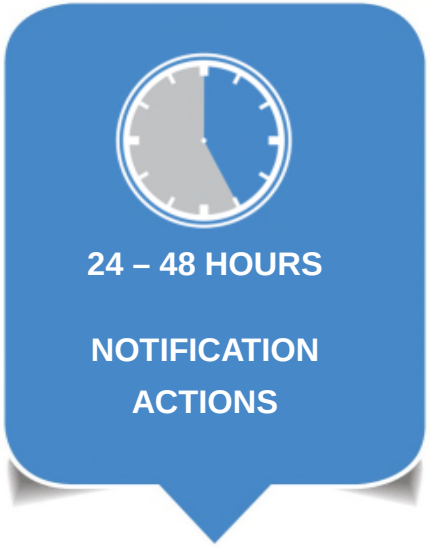
- Retain data, preserve evidence
- Forensic analysis and initial assessment
- Steps to contain breach
- Steps to maximise business resilience / continuity e.g.
  - taking systems down
  - cutover to backup systems/data

A response timeline cont.

Risk evaluation and communication

- Critical supplier communications e.g. evidence preservation letters to service/cloud providers
- Critical customer communications
- Information/Evidence gathering
- Statements from relevant representatives
- Develop a PR strategy
- Internal and External comms/PR releases (if sufficient information known and rectification)

A response timeline cont.



Notification/Consultation Actions – 24 to 48 hours

- *Regulatory:*
  - Mandatory notices to regulators/affected individuals required? Australia only?
  - Voluntary consultation e.g. APRA?
- *Industry:* e.g. CERT, AFP?
- *Contractual* – contractual obligations to disclose?

First party / Third party claims assessment

- Initial assessment of potential claims available against third parties, e.g. third party supplier contract breach
- Initial assessment of internal costs/losses
- Initial assessment of exposure to third parties e.g. customers, regulators

A response timeline cont.

Post-Incident – Implement key learnings

- Consider the need to:
  - Update incident response plan
  - Update members of the ICT
  - Change internal systems, processes, policies
  - Adopt alternative risk positions in customer / supplier arrangements

TECHLAW AUSTRALIA

Melbourne

Thursday, 22 June 2017