Regulatory Failure in the Security Space: Some Current Cases

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor in Computer Science, ANU, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney

http://www.rogerclarke.com/DV/RFSS {.html, .pdf}

Crime and Justice Research Centre
QUT – 12 September 2016

The Notion of Security

A condition
in which harm does not arise
despite the occurrence of threatening events

A set of safeguards
whose purpose is
to achieve that condition

The Conventional Security Model
Key Concepts

- A **Threat** is a circumstance that could result in Harm

  A **Threatening Event** is an instance of a generic Threat

  A Threat may be natural, accidental or intentional

  An intentional Threatening Event is an **Attack**

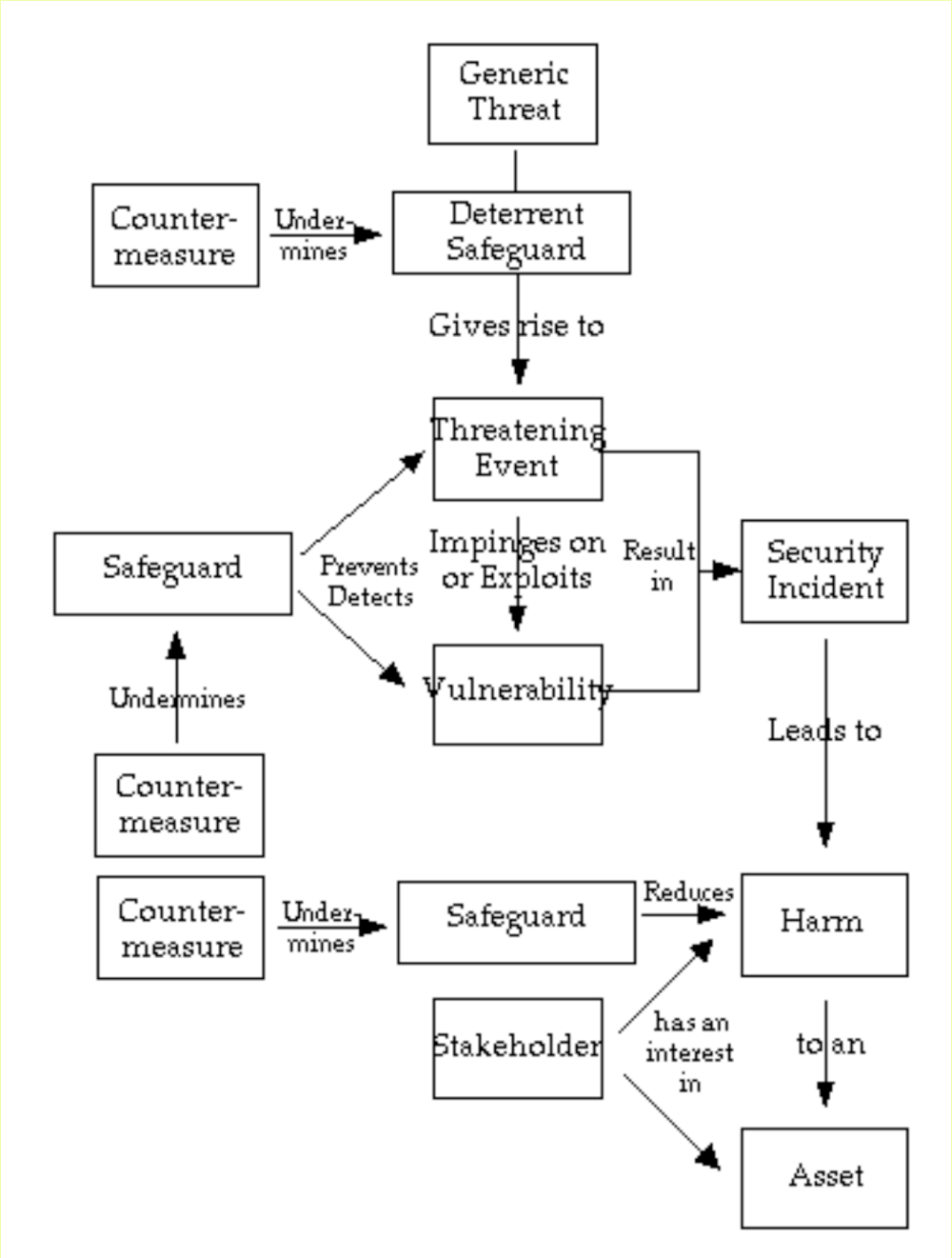
  A party that creates an Intentional Threat is an **Attacker**

- A **Vulnerability** is a susceptibility to a Threat
- **Harm** is any kind of deleterious consequence to an **Asset**

- A **Safeguard** is a measure to counter a Threat
- A **Countermeasure** is an action to circumvent a Safeguard

XAMAX Consultancy Pty Ltd

The Conventional Security Model



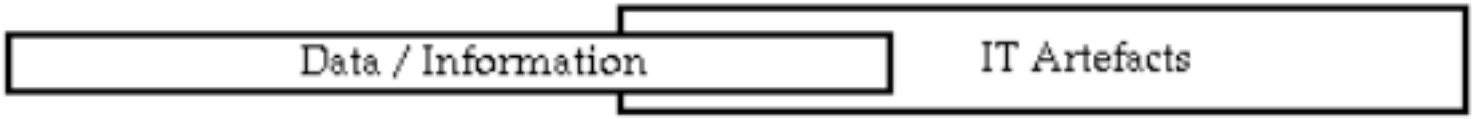
http://www.rogerclarke.com/EC/PBAR.html#App1

Asset, Harm, Value, Stakeholder

- **Harm** means deleterious impact on an **Asset**
- But which Harm matters, to which Assets?
- That depend on the perspective that's adopted and the **Values** that are perceived in Assets
- So it's necessary to define **Stakeholders**

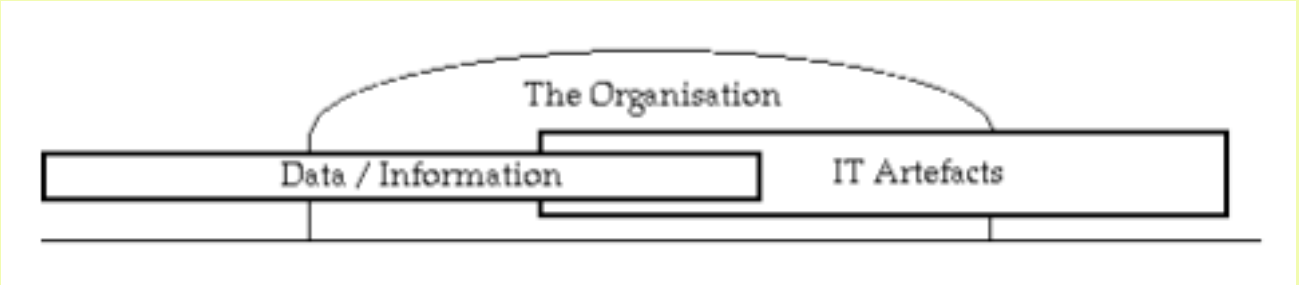
'Whose Security?'

The Scope of Security



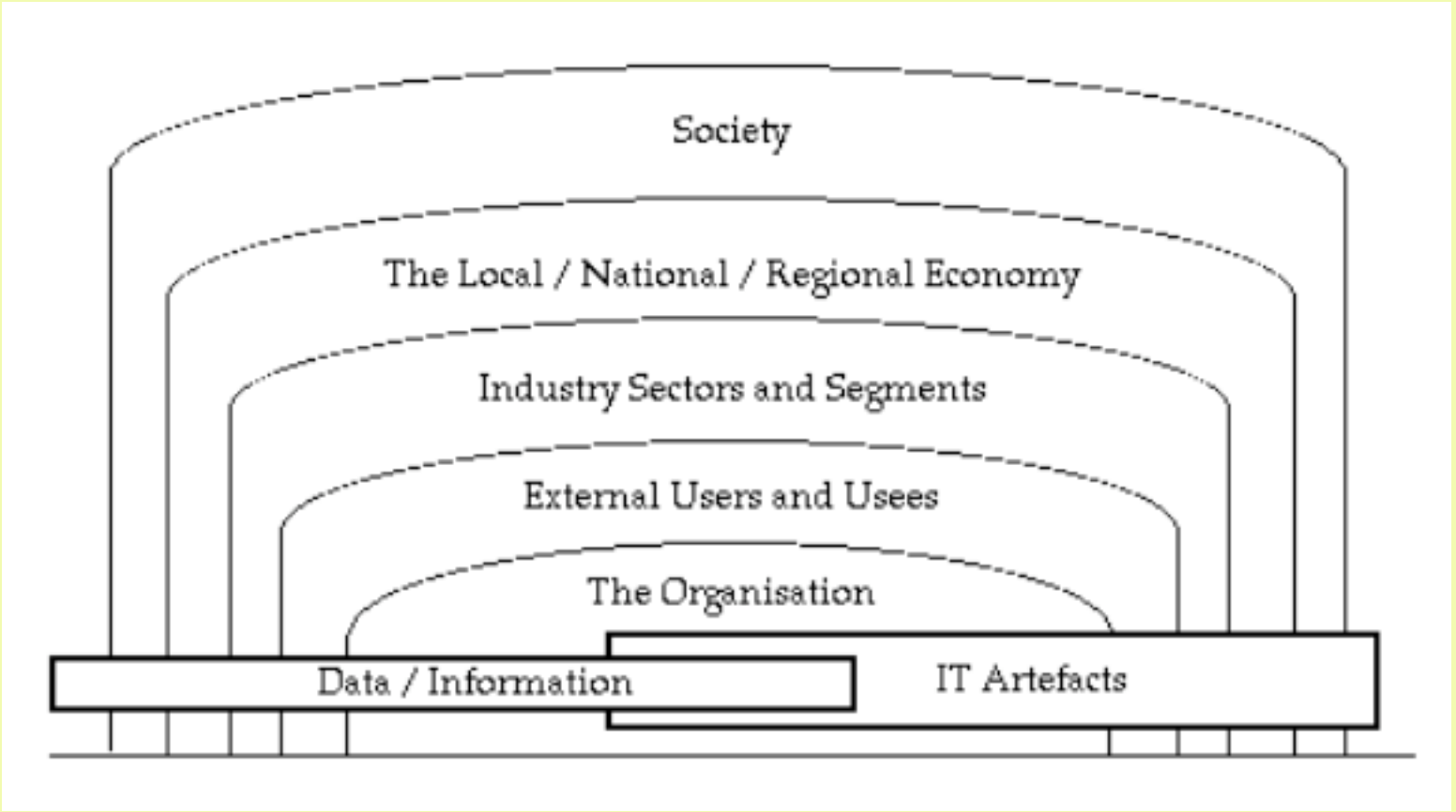
XAMAX Consultancy Pty Ltd

The Organisational Scope of Security



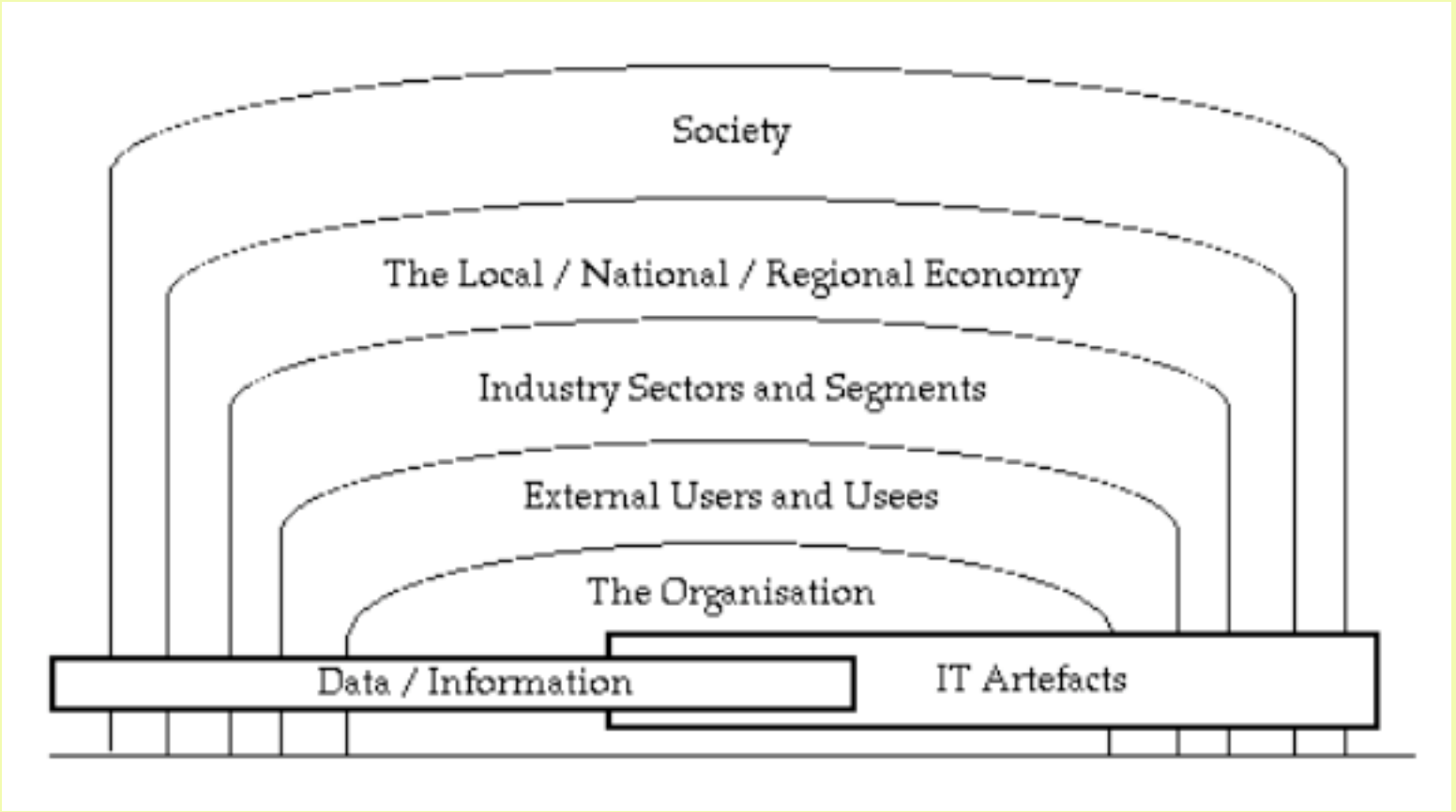
XAMAX Consultancy Pty Ltd

The Many Scopes of Security



XAMAX Consultancy Pty Ltd

And where is 'National Security'?



XAMAX Consultancy Pty Ltd

Is this 'National Security'?

The protection of a nation from attack or other danger by holding adequate armed forces and guarding state secrets

Encompasses economic security, monetary security, energy security, environmental security, military security, political security and security of energy and natural resources

http://definitions.uslegal.com/n/national-security/

"specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy"

US Freedom of Information Act

Or is this 'National Security'?

- **Critical Infrastructure Security**
  Bombs in ports, ships, railways, energy, ...
  Anthrax in the water supply, ...

- **Public Safety**
  Bombs in aircraft, mayhem in marketplaces
  Major Events, e.g. 'The Euros', The Olympics

- **Prominent Person Safety**
  Bush and Blair; Rushdie and Kurt Westergaard
  Gx, APEC, CHOGM, ...

'Terrorism'

The use of violence or the threat of violence,
especially against civilians,
in order to alarm the public,
in the pursuit of political [or politico-religious] goals

'Terrorism' has been conflated with 'National Security'

2. The Regulatory Framework

Forms: / Actors:	**Formal Regulation** ('Government')	**Co-Regulation**	**Industry Self-Regulation**	**Organisational Self-Regulation** ('Governance')
The State	**Determines What and How**	**Negotiates What and How**	Influences What	Has Limited Influence
Industry Assocn	Influences What and How	**Negotiates What and How**	**Determines What and How**	Influences What and How
Corporations	Contribute to Industry Assocn	Contribute to Industry Assocn	Contribute to Industry Assocn	**Determine What and How**
Other Stakeholders	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence
	Statutes & Delegated Legislation	Statutory Codes & Standards	Industry Codes & Standards	Customer Charters

How to Recognise
An Effective Regulatory Scheme

Process

- Clarity of Aims, Requirements
- Transparency
- Participation
- Reflection of Stakeholder Interests

Product

- Comprehensiveness
- Parsimony
- Articulation
- Educative Value
- Appropriate Generality and Specificity

Outcomes

- Oversight
- Enforceability
- Enforcement
- Review

3. Some Test-Cases

1. **PIAs for National Security Initiatives**
2. Big Data Analytics
3. The 'Internet of Things' ...
4. Remotely-Piloted Drones
5. Autonomous Cars
6. The EC GDPR's DPIA
7. The Precautionary Principle

'Terrorism' and National Security
The Australian Context

- **Each decade pre 2000 saw some such event(s)**
- 2002 – 88 Australian deaths in Bali,
  at a nightclub frequented by Australians
- **Deaths – 2000's (0), 2010s (1)**
- **2015 – 1 domestic murder by a 15yo 'lone wolf'**
  That's the sole death in Australia since 2001
- Several credible claims of interdiction 2001-15
- But periodic large-scale raids come up near-empty:
  successful prosecutions of only 15 individuals
  re 6 instances of preparation to commit an act (+ 1!)

https://www.crikey.com.au/2014/09/04/
the-real-threat-of-terrorism-to-australians-by-the-numbers/
http://www.abc.net.au/news/2015-02-25/
fact-file3b-five-facts-about-terrorism-in-australia/6226086
https://www.start.umd.edu/gtd/search/Results.aspx?country=14

XAMAX Consultancy Pty Ltd

National Security Measures Since 2001 Have Compromised Many Human Rights

- Freedom from Arbitrary Detention (ICCPR Art. 9)
- Freedom of Movement (Art. 12)
- Right to a Fair Trial (Art. 14.1), Minimum Guarantees in Criminal Proceedings (Art.14.2-14-7)
- Privacy (Art.17)
- Freedom of Information, Opinion, Expression (Art. 19)
- Freedom of Association (Art. 22)
- Other Rights Potentially at Risk (Arts. 2.1, 7, 15, 21, 24, 26, 27)

http://www.rogerclarke.com/DV/IANS.html#App4

Extracted from AHRC (2008), Williams (2011), HRLC (2011, 2012) LCA (2012), Lynch et al. (2014)

Evaluation Meta-Principles

Pre-Conditions

1. Evaluation
2. Consultation
3. Transparency
4. Justification

Design

5. Proportionality
6. Mitigation
7. Controls

Post-Condition

8. Audit

Whose Security? A Case Study
PIAs and National Security in Australia

Privacy Impact Assessment

- a systematic process, which ...
- identifies and evaluates ...
- from the perspectives of all stakeholders ...
- the potential effects on privacy of ...
- a project, initiative or proposed system or scheme
- and which includes a search for ways to avoid or mitigate negative privacy impacts

Reasons to do a PIA

- **Surfacing and Examination** of the privacy impacts and implications of a proposal
- **Development of a clear understanding of the Business Need that justifies the proposal and its negative impacts**
- **Gauging of the Acceptability** of the proposal and its features by organisations and people that will be affected by it
- [**Assessment of Compliance** of the proposal with existing privacy-related laws, codes, best practices and guidelines]
- Constructive Search for, and Evaluation of, better **Alternatives**
- **Constructive Search for ways to Avoid Negative Impacts, and ways to Mitigate Unavoidable Negative Impacts**
- Documentation and Publication of the **Outcomes**

'Privacy Impact Assessment: Its Origins and Development'
Computer Law & Security Review 25, 2 (April 2009) 123-135
http://www.rogerclarke.com/DV/PIAHist-08.html

3.1 A Five-Factor Test of the Efficacy of a PIA

1. Is there evidence of a PIA process being **performed**?
2. Were advocacy organisations **aware** of that process?
3. Did the project sponsor(s) **engage** with advocacy organisations?
4. Was the PIA **Report published** on completion?
5. Were advocacy organisations' views appropriately **reflected** in the PIA Report?

   However, it was known that there was a low incidence of published Reports. Hence:

6. Did the PIA **Report come to light** later, e.g. as a result of an FoI request by the media?

PIAs don't operate as a Control Mechanism over Australian National Security Initiatives

AGD

- **Passed** the 5-factor test **2/36**
- Engagement with advocacy organisations 3/36 (but their views were ignored)
- Secret (hence flawed) PIA processes 10/36

Other Agencies

- **Passed** the 5-factor test **1/36**
- Engagement with advocacy organisations 5/36

Case Studies

1. **Document Verification System (DVS) 2004-15**
   Some PIAs, but advocates were excluded, and
   the 2014-15 expansion was done entirely in secret
2. **ANPR Mass Surveillance 2007-**
   Reneged on publication of the PIA report
   Committed to PIA processes, but did no more
3. **Telecommunications Act s.313 2013-15**
   Impenetrable text secretly interpreted to mean that a 'request' for assistance from a telco or an ISP imposes a positive obligation – any agency, any purpose, no warrant, no controls. And no PIA or other consultation
4. **(Meta-)Data Retention 2003-15**
   No PIA was ever performed, and submissions
   by 30 advocacy organisations were ignored

Conclusions about PIAs and NatSec

- 3 of the 72 projects (4%) passed every test
- 57 of the 72 projects **(79%) failed every test**
- **AGD has continually breached expectations, public policy and arguably the law, but has avoided publicity and suffered no sanctions**
- 7 advocacy organisations wrote jointly to the AG in September 2011. No reply was received
- The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is a puppet
- The Privacy Commissioner is a captive
- **PIAs <u>don't</u> operate as a Control Mechanism over Australian National Security Initiatives**

XAMAX Consultancy Pty Ltd

Why Not?
The Reasons for Organisations Not to Do a PIA

- Cost
- Delay
- Information Disclosure about the Organisation's Activities
- Opportunity for Opponents to achieve countervailing power

Regulatory Failure is Evident

- Organisations don't undertake evaluation processes that reflect multiple Stakeholders' interests
- So the requirement has to be imposed from without
- But Executives and Legislatures focus on stimulatory measures, not on ensuring appropriate controls and mitigation measures are in place

4. Conclusions

Policy Perspective

- Executives and Legislatures need to be forced to perform their functions, and ensure effective regulation of potentially harmful behaviours

Research Perspective

- More and deeper case studies
- Process studies in insecurity
- Studies of effectiveness of particular safeguards

Regulatory Failure in the Security Space: Some Current Cases

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor in Computer Science, ANU, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney

http://www.rogerclarke.com/DV/RFSS {.html, .pdf}

Crime and Justice Research Centre
QUT – 12 September 2016