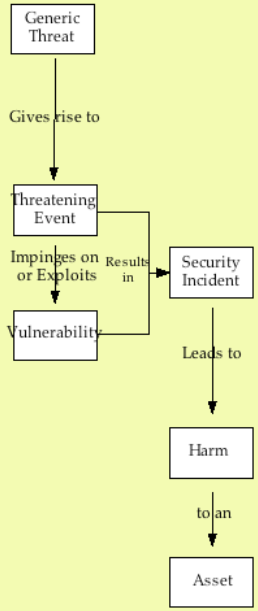
Managing Data Risk
A Consultant's Guide

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor, ANU RSCS and UNSW Law

http://rogerclarke.com/EC/MDR.html
http://rogerclarke.com/EC/MDR.pdf

ANU CyberLaw Program – 12 Aug 2020

The Conventional Security Model

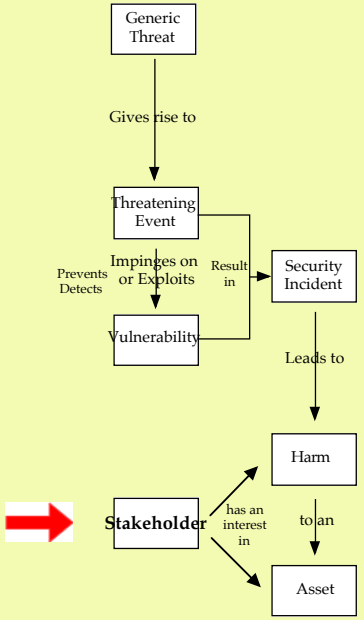


http://rogerclarke.com/EC/SSACS.html#App1

Categories of Threat

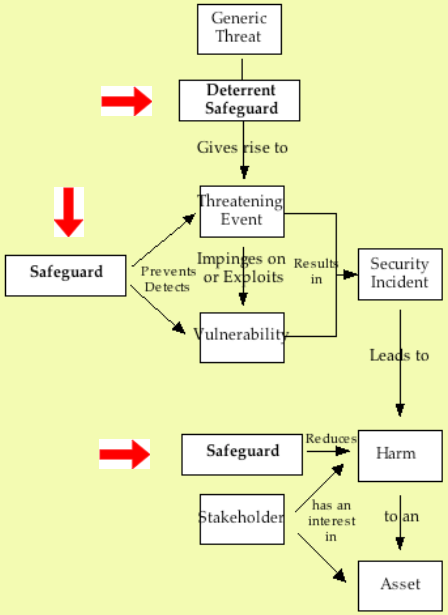
- **Environmental Events** (Acts of Gods or Nature)
- **Accidents**, caused by:
  - Humans who are directly involved
  - Other Humans
  - Artefacts and those Responsible for them
- **Attacks**, by:
  - Humans who are directly involved
  - Other Humans
  - Artefacts and Designers, Owners, Operators

The Conventional Security Model + Stakeholder



http://rogerclarke.com/EC/SSACS.html#App1

The Conventional Security Model + Safeguards



http://rogerclarke.com/EC/SSACS.html#App1

Deterrent and Preventative Safeguards

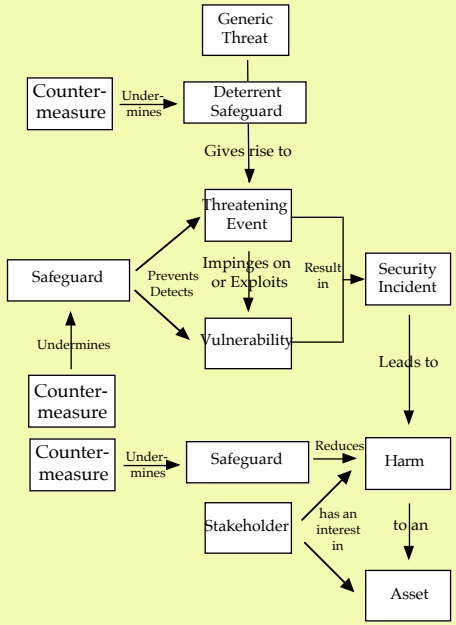
Lightning strikes and bush-fires not permitted at this installation

Deterrent and Preventative Safeguards

Lightning strikes and bush-fires not permitted at this installation

CROCODILE-INFESTED SWAMP
Survivors will be prosecuted

The Conventional Security Model



http://rogerclarke.com/EC/SSACS.html#App1

Attacks

By Whom?

Principals

- Opportunists
- Hacktivists
- Vigilantes
- Organised Crime
- Corporations
- Nat Sec Agencies
- Nation-States

Agents

- Mercenaries

Why?

Politics

- Protest against action
- Retaliation / Revenge
- Public Safety / Nat Sec
- Espionage

Economics

- Financial Gain
- Financial Harm

Social/Cultural Factors

- Challenge
- Dispute
- Celebration

Summary of Key Terms

- **Threat**
  A circumstance that could result in Harm
- **Vulnerability**
  A susceptibility to a Threat
- **Threatening Event**
  An occurrence of a Threat
- **Safeguard**
  A measure to prevent, to enable detection or investigation of, or to mitigate Harm from, a Threatening Event
- **Risk**
  "The likelihood of Harm arising from a Threat"
  A measure of the likelihood and/or seriousness of Harm arising from a Threatening Event impinging on a Vulnerability and not being dealt with satisfactorily by the existing Safeguards

Risk Assessment and Risk Management Processes

1. Analyse / Perform Risk Assessment
1.1 Define the Objectives and Constraints
1.2 Identify the relevant Stakeholders, Assets, Values and categories of Harm
1.3 Analyse Threats and Vulnerabilities
1.4 Identify existing Safeguards
1.5 Identify and Prioritise the Residual Risks
2. Design / Prepare for Risk Management
2.1 Identify alternative Safeguards
2.2 Evaluate the alternatives against the Objectives and Constraints
2.3 Select a Design or adapt alternatives to achieve an acceptable Design
3. Do / Perform Risk Management
3.1 Plan the implementation
3.2 Implement
3.3 Review the implementation

Forms of Value in Data Assets

- **Intrinsic Value**
  Debtors Ledgers, Share Registers, Land Registers
- **Operational Value**
  Usefulness for Inventory Management
- **Competitive Value**
  Usefulness to the organisation and its competitors
- **Reputational Value**
  Capacity to influence perceptions of the organisation
- **Compliance Value**
  Usefulness for fulfilling legal obligations
- **Personal Value**
  The data subject's ec/soc/psych interests

Categories of Harm to Data Assets

- **Inaccessibility (Confidentiality)**
  - Data Access
  - Data Disclosure
  - Data Interception
- **Quality (Integrity)**
  - Data when Collected
  - Data when Used
    - Modification
    - Corruption
    - Staleness
- **Accessibility (Availability)**
  - Data Existence
  - Data Loss
    - In Volatile Memory
    - In Non-Volatile Memory
    - Theft, Destruction, Malfunction
  - Data Inaccessibility

Categories of Compliance-Related Harm

- **General Statutory & Common Law Obligations**
  - Evidence Discovery Law
  - Financial Regulations
  - Directors' obligations re asset protection, due diligence, business continuity, risk management
  - Security Treaty Obligations
- **Confidentiality**
  - Corporate Strategic and Commercial
  - Governmental
- **Privacy**
  - Unauthorised Use, Disclosure / Data Breach
  - Storage in Data Havens

Multi-Stakeholder Risk Assessment and Risk Management

1. Analyse / Perform Risk Assessment		
1.1 Define the Objectives and Constraints		
1.2 Identify the relevant Stakeholders		
Organisational Risk Assessment	**Stakeholder A Risk Assessment**	**Stakeholder B Risk Assessment**
O1.3 Review Objectives, Constraints	A1.3 Define Objectives, Constraints	B1.3 Define Objectives, Constraints
O1.4 Assets, Values, Harm	A1.4 Assets, Values, Harm	B1.4 Assets, Values, Harm
O1.5 Threats, Vulnerabilities	A1.5 Threats, Vulnerabilities	B1.5 Threats, Vulnerabilities
O1.6 Existing Safeguards	A1.6 Existing Safeguards	B1.6 Existing Safeguards
O1.7 Residual Risks	A1.7 Residual Risks	B1.7 Residual Risks
2. Design / Prepare for Risk Management		
2.1 Identify alternative Safeguards		
2.2 Evaluate the alternatives against the Objectives and Constraints		
2.3 Select a Design or adapt / refine the alternatives to achieve an acceptable Design		
3. Do / Perform Risk Management		
3.1 Plan the implementation		
3.2 Implement		
3.3 Review the implementation		

Categories of Risk Management Strategy

- **Proactive Strategies**
  - Avoidance
  - Deterrence
  - Prevention
  - Redundancy
- **Reactive Strategies**
  - Detection
  - Reduction /Mitigation
  - Recovery
  - Insurance
- **Non-Reactive Strategies**
  - Tolerance / Self-Insurance
  - Graceful Degradation
  - Graceless Degradation

Irresponsible Data Analytics
Robo-Debt

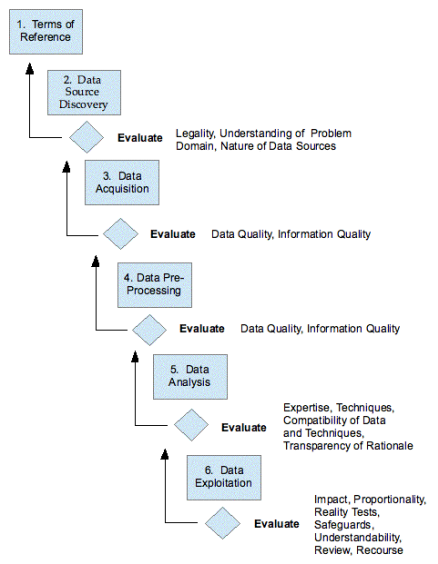
Australian Government
Australian Taxation Office

Australian Government
Services Australia

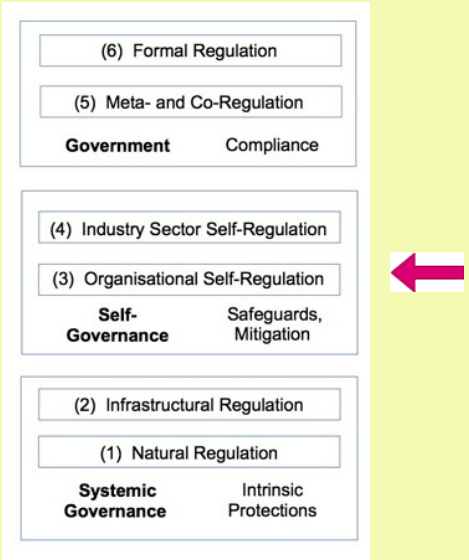
- **ATO** collects data relating to the financial year
- **Centrelink** relies on more finely-grained data: the fortnightly income of each welfare client
- **Centrelink divided ATO's annual figure by 26, and assumed it applied to each fortnight**
- **Centrelink inferred that many clients had mis-reported their income and been overpaid**
- **Centrelink declared those people owed money**
- x30 Leap in case-load, so complaints were ignored
- Centrelink hired heavy-handed debt-collectors
- ***People suffered badly for 3 years as a result***
- ***The program was in clear breach of the law***
- ***Cost to the public purse $1 billion and rising***

Responsible Data Analytics

A Business Process Model



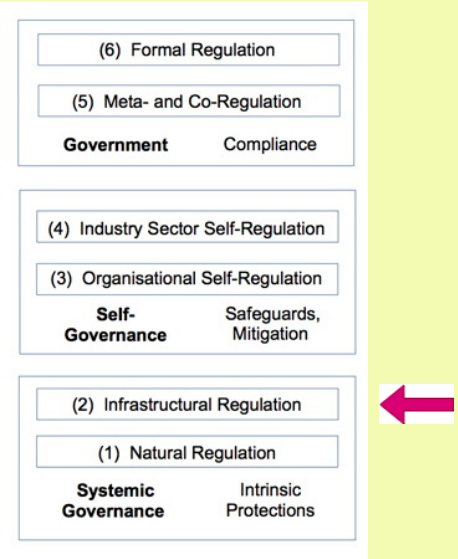
The Hierarchy of Regulatory Forms



A View of Self-Regulation

Wolves herd sheep
not for the benefit of the sheep
but for the benefit of the wolves

The Hierarchy of Regulatory Forms



Infrastructural Regulation

- The mechanical steam governor
- Reinforce positive aspects, Inhibit negatives
- Automated ... Monitoring, Exception condition detection, Adjustment of parameters, Deployment of countermeasures, Suspension of activities
- Byproduct, Retro-fitted on, or Architected in

- Dam sluice-gates automatically adjust to water-level, water-flows, precipitation events
- Lessig's 'West Coast Code' – computer and network architecture, standards and protocols
- 'The {Extended} Laws of Robotics'

Managing Technology-Associated Risk

- The Conventional Security Model
- Risk Assessment
  - Processes
  - Applications
- Risk Management
  - Processes
  - Choices
- A Hierarchy of Regulatory Forms

Managing Data Risk
A Consultant's Guide

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor, ANU RSCS and UNSW Law

http://rogerclarke.com/EC/MDR.html
http://rogerclarke.com/EC/MDR.pdf

ANU CyberLaw Program – 12 Aug 2020