Managing Technology-Associated Risk

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor, ANU RSCS and UNSW Law
http://rogerclarke.com/EC/MTAR.html
http://rogerclarke.com/EC/MTAR.pdf

ANU CyberLaw Program – 11 May 2020

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

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

The Conventional Security Model + Stakeholder

http://rogerclarke.com/EC/SSACS.html#App1
The Conventional Security Model + Safeguards

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

Counter-measure Undermines
Safeguard Prevents or Exploits Vulnerability

Generic Threat
Deterrent Safeguard

Threatening Event

Lightning Incident

Safeguard

Harm

Stakeholder

Asset
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

---

Locations of Security Risks

- **1st Person** – **Users, User Organisations**
  Vulnerable Devices, Software & Infrastructure, User Threats

- **2nd Person** – **Their Business Partners, Service Providers**
  Abuse, Vulnerable Storage, Infrastructure, User Threats

- **3rd Person** – **Their Business Partners, Service Providers, Others**
  Access
  Abuse, Vulnerable Storage, Infrastructure, User Threats

---

Risk Assessment and Risk Management Processes

1. Analyse / Perform Risk Assessment
   1. Define the Objectives and Constraints
   2. Identify the relevant Stakeholders, Assets, Values and categories of Harm
   3. Analyse Threats and Vulnerabilities
   4. Identify existing Safeguards
   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

---

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
A Generic Data Risk Assessment of Cloudsourcing

- **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

= Multi-Stakeholder Risk Assessment and Risk Management

---

Categories of Risk Management Strategy

- **Proactive Strategies**
  - Avoidance
  - Deterrence
  - Prevention
  - Redundacy

- **Non-Reactive Strategies**
  - Tolerance / Self-Insurance
  - Graceful Degradation
  - Graceless Degradation

- **Reactive Strategies**
  - Detection
  - Reduction / Mitigation
  - Recovery
  - Insurance

---

An Example: A Business Process Model for Responsible Data Analytics Projects
IRresponsible Data Analytics
Robo-Debt

- 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

The Hierarchy of Regulatory Forms

(6) Formal Regulation
Government Compliance

(5) Meta- and Co-Regulation

(4) Industry Sector Self-Regulation

(3) Organisational Self-Regulation
Self-Governance Safeguards, Mitigation

(2) Infrastructural Regulation

(1) Natural Regulation
Systemic Governance Intrinsic Protections

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

(6) Formal Regulation
Government Compliance

(5) Meta- and Co-Regulation

(4) Industry Sector Self-Regulation

(3) Organisational Self-Regulation
Self-Governance Safeguards, Mitigation

(2) Infrastructural Regulation

(1) Natural Regulation
Systemic Governance Intrinsic Protections

http://www.rogerclarke.com/DV/CRD17.html

http://rogerclarke.com/EC/AIR.html#RF
Managing Technology-Associated Risk

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

Managing Technology-Associated Risk

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

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

ANU CyberLaw Program – 11 May 2020