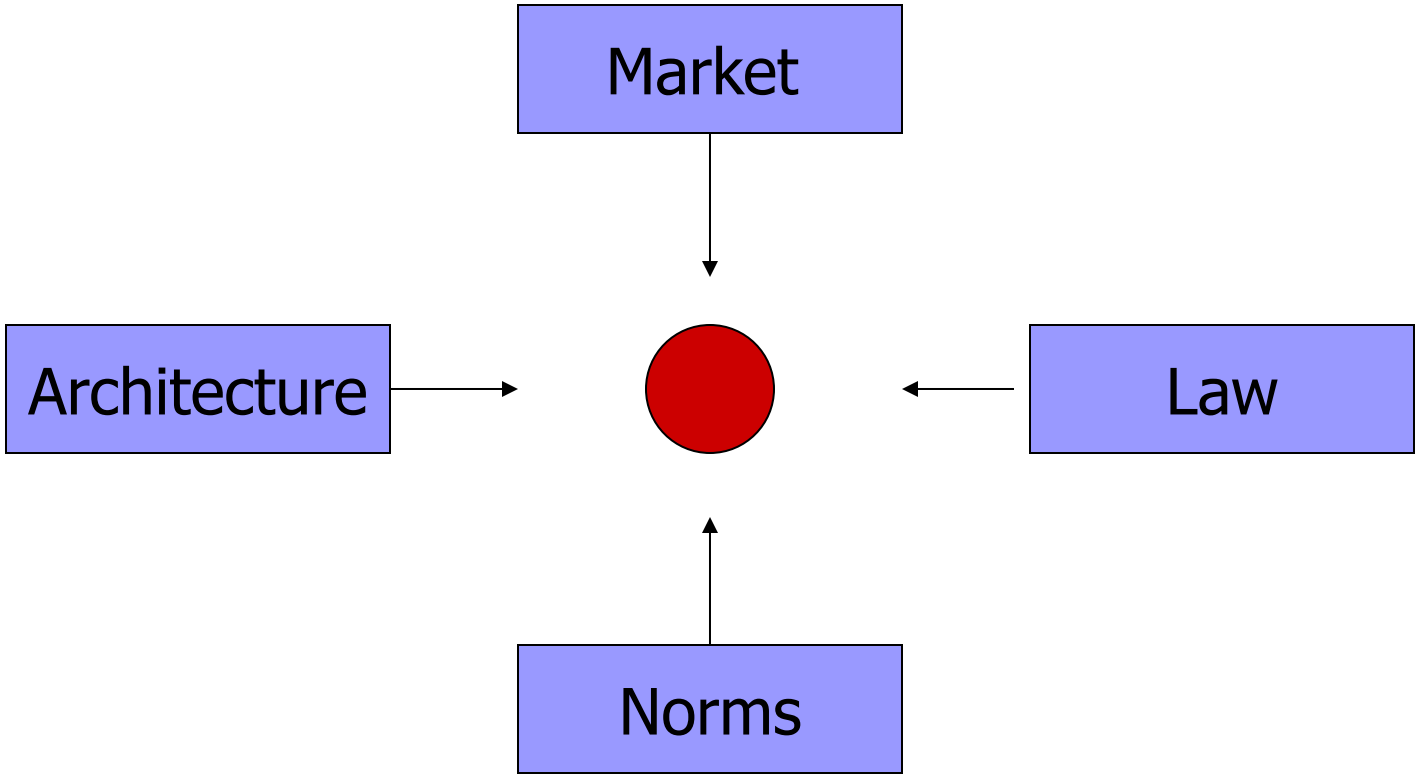
MARK HEYINK

Cybercrime and Cybersecurity Bill

Cape Town

10th November 2015

ICE



Prof. Lawrence Lessig

Cybersecurity- Non-negotiable

- Called for legislative in 2002
- Practical issues remain unaddressed
- Little capacity or competence in Govt

NCPF

- Product of SSA
- Draft published 2010
- Passed by Cabinet 2012
- De-classified October 2015

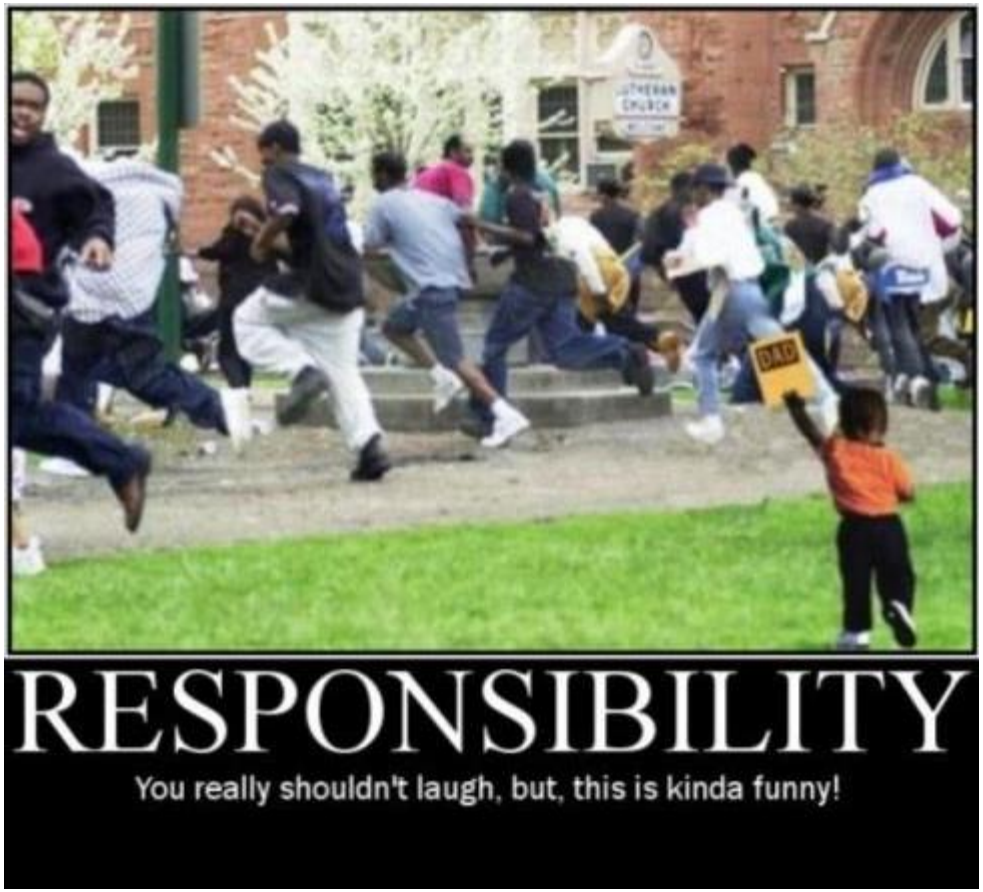
Legal framework

- Does not say who?- DOJ has been given this responsibility
- National Cybersecurity implementation plan
- Privacy- a constitutional right- is not mentioned in Executive Summary

Novelty

- New challenges
- Cybersecurity culture driven by the state ???
- SA out of line with open democracies

NCPF responsibilities



- Govt led integrated approach
- Promote cybersecurity culture
- PPPs
- Protection of critical infrastructure
- Comprehensive legal framework

Purpose

- Enable development of information society-
- Fundamental rights:
  - Privacy
  - Security
  - Dignity, access to information
  - Communication and free speech

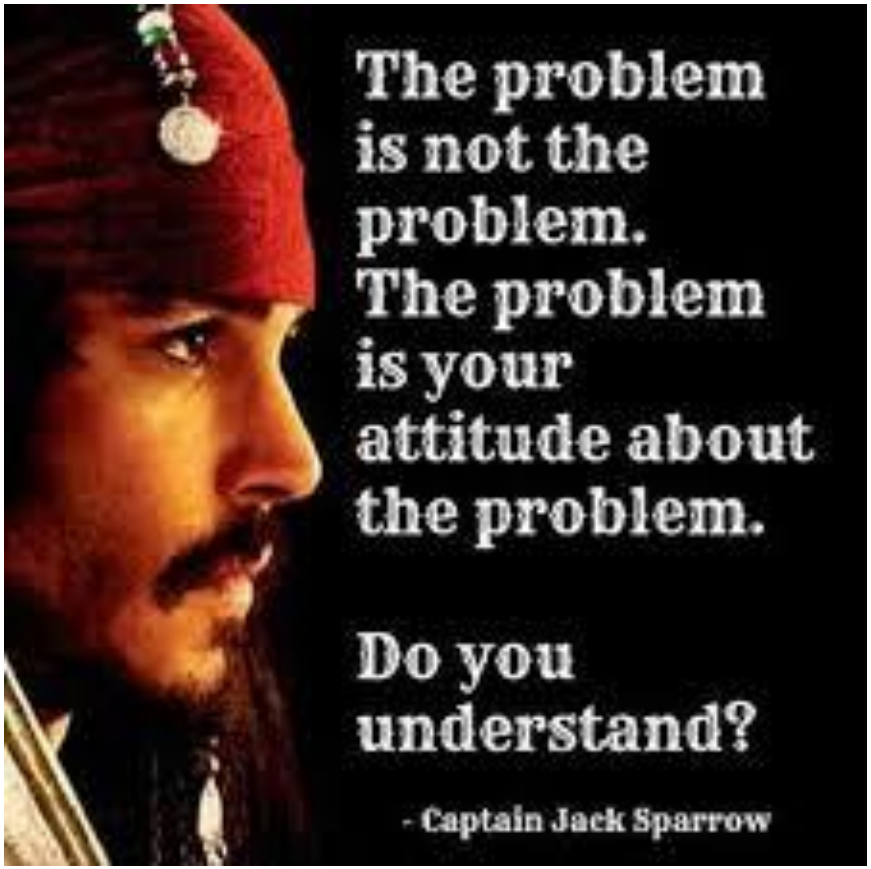
Other matters

- Verification of security products
- NCII Protection
- Cryptography
- Online E-Identity
- Cooperation
- Capacity development

Cybersecurity Culture

- Why have there been such delays with POPI?
- Cannot have cybersecurity laws without privacy laws

Bill



- Three primary problems
  - Consultation- out of line with international models
  - PPPs nothing assists in establishment of PPPs
  - Privacy- not recognised

Chapter 2 Offences

- Creates several new offences
- “Computerises” old offences
- Shifts onus of proof

I personally would suggest government. They never go to jail.

Sect 2 Offences

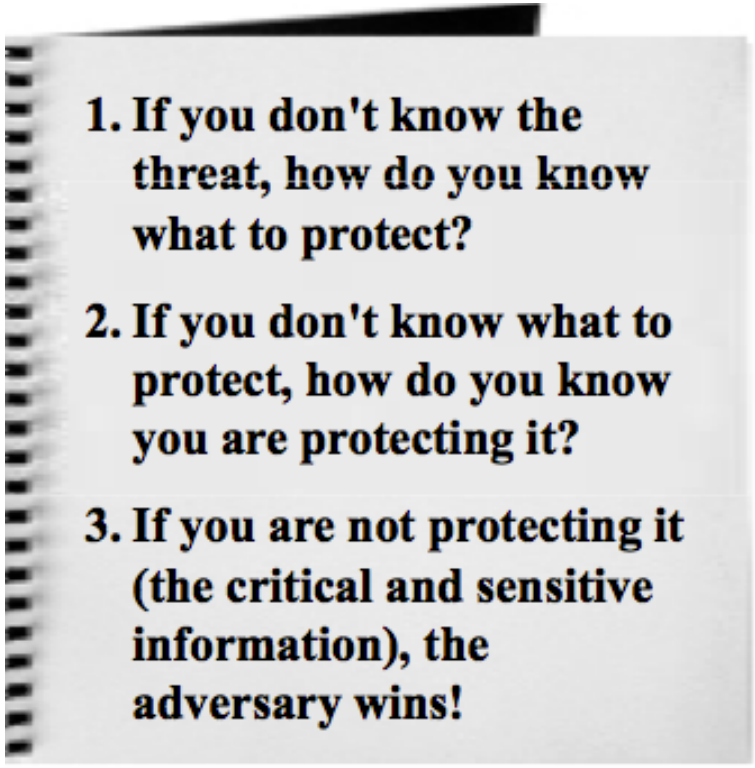
- "Written authority"- Lawful
- Exceeds written authority- **must** be regarded as unlawful

Sect 3 Personal Information

- Perverts POPI
- No accommodation of regulator
- Financial Information
- Should increase penalties in POPI and delete this provision from the Bill

Sect 6: Hardware and Software

- Possession and use
- Reasonable suspicion
- Satisfactory exculpatory account
- Technology is neutral, how we use it determines its nature
- Shift of onus



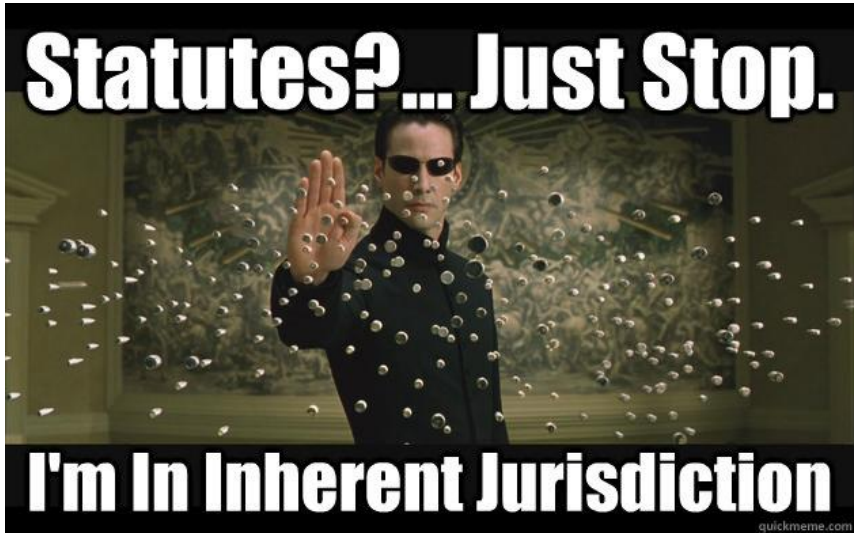
Sect 9 Malware

- Dolus Eventualis
- Reasonable suspicion
- Unable to give a satisfactory exculpatory account
- Shifts onus
- SAP incompetence

Sect 10 Passwords et al

- Remain the keys
- Typically poor
- What are the tech problems that occur?
- Where does responsibility on system owner lie?

Chapter 3 Jurisdiction



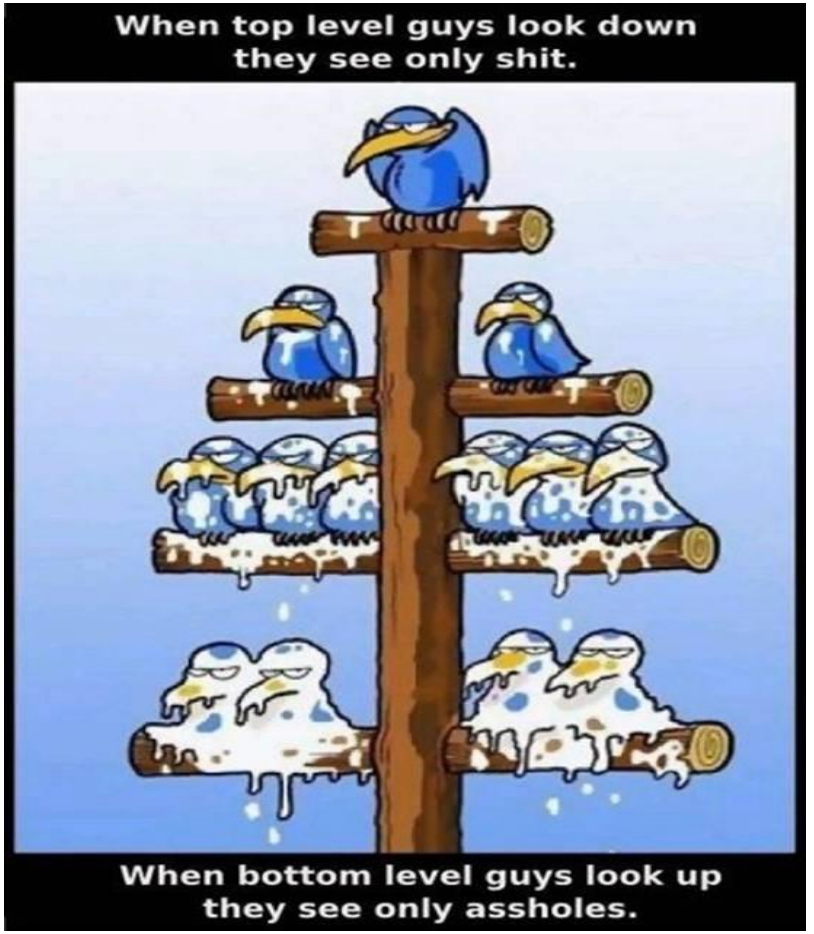
- Problematic internationally
- Widening of ambit of jurisdiction
- Effectiveness will depend on international co-operation

Chap 4: Powers of Law Enforcement

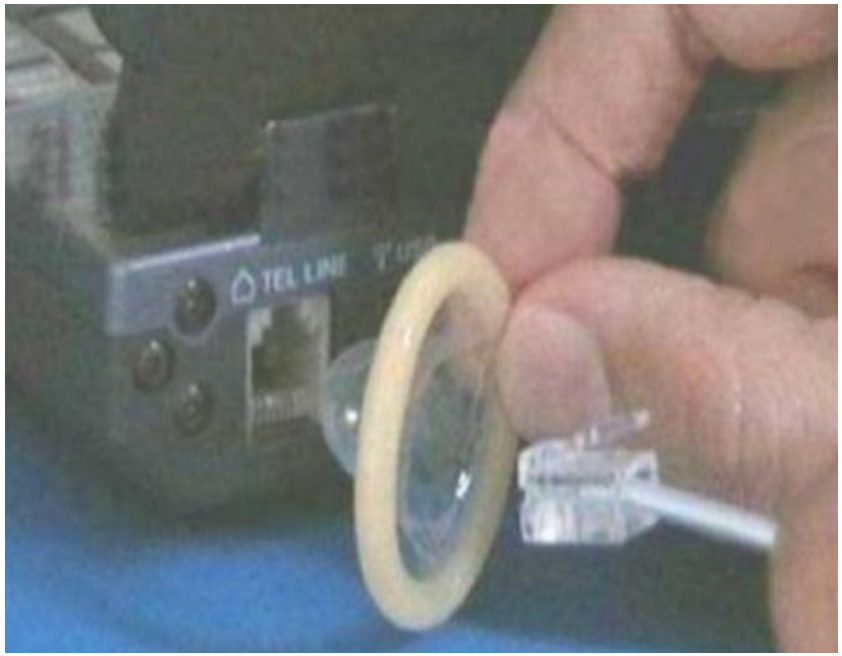
- Heavily biased towards law enforcement
- No privacy protections
- Erodes civil liberties
- Safe harbour accord?

Chap 5&6: Cybersecurity Structures

- Fragmented
- SSA- chief asshole
- Several of the govt departments do not have capacity
- PPPs poorly dealt with



Chap 7: NCII Protection



- Govt to set minimum information security standards
- MISS
- Cost for private sector
- Offences if not complied with
- Capacity and Competence

Chap 8: Evidence

- SALRC
- Discussion paper on evidence ignored
- Badly drafted as is sect 15(4) of ECT Act.

Comment

- Please be pro-active
- This bill has the same potential for harm as the secrecy bill

MARK HEYINK

Thank You!

The incidents related and examples provided in this presentation are based on fact, only names and dates have been changed to protect innocent (and not so innocent) people involved.

Mark Heyink

mark@heyink.co.za

Tel 011 454 0449

Fax 011 454 0036

Cell 082 904 3774