steria

bcs The Chartered Institute for IT
Hertfordshire Branch

Information Security: Why is it so hard?

Philip Le Riche - Steria Ltd

In the beginning… (or shortly after)

Elliott 803B www.tnmoc.org

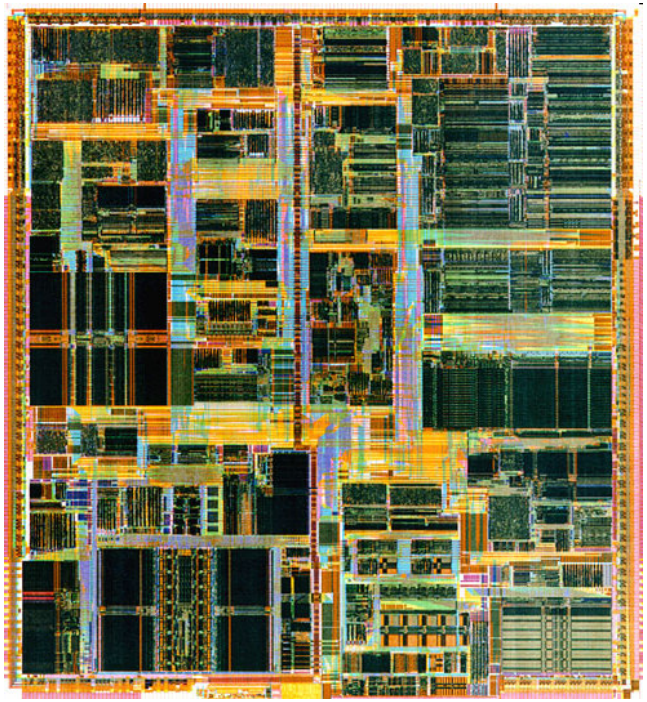
1960's: RAM: 40kB; CPU: Serial, 1500 gates, 1KFLOP;
backing store: comparable to audio cassette;
Comms: None.

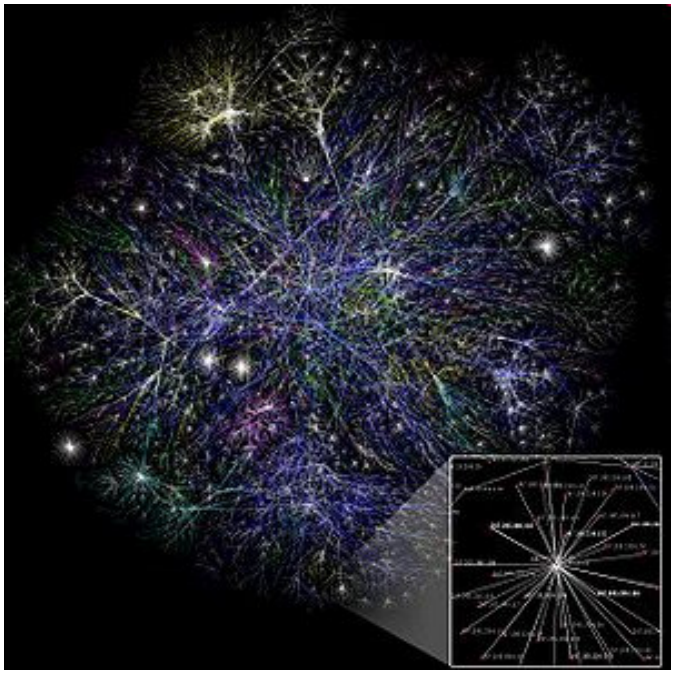
… the plot thickens …

ICL 2966 www.tnmoc.org

70’s - 80’s: Multi-access arrives!

… things get serious.





80’s – 90’s:

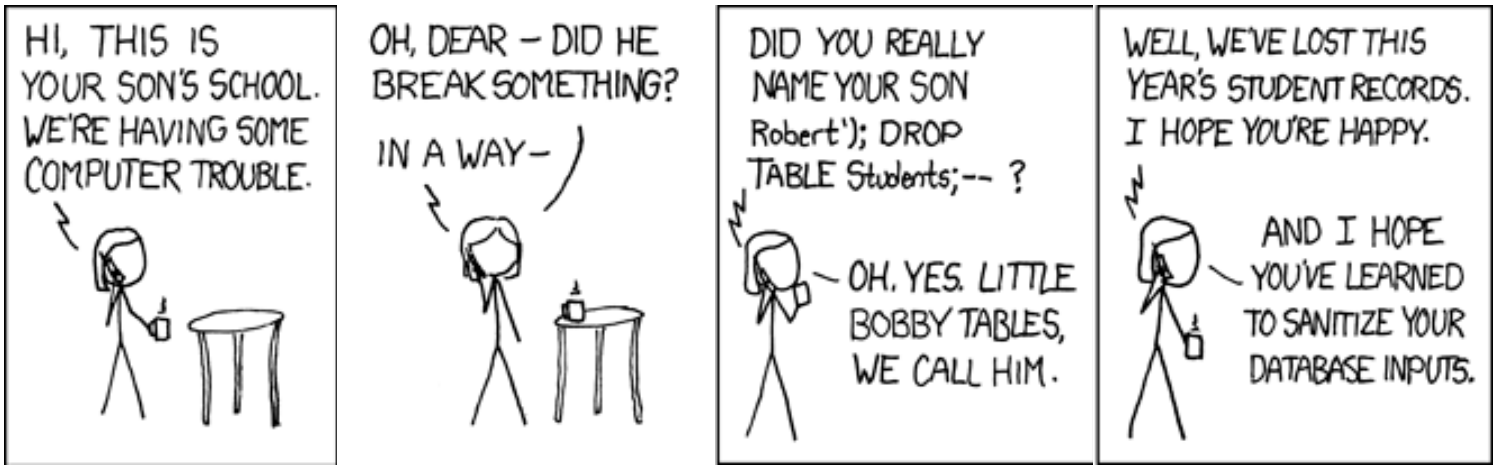
The semiconductor revolution + The Internet

vs Security

Where are we today? Vulnerabilities

- Vulnerabilities
  - Operating Systems
  - Applications
  - The Web
  - Protocols
  - The Wetware

SQL Injection



SQL Injection

Where are we today? Threats

Threat Sources

Crime

FIS

Industrial Espionage

Threat Vectors

Spam

Malware

Compromised websites

Exploit toolkits

Botnets

Where are we today? Risks

Risks

Risk = Threat + Vulnerability

Data loss

Fraud

Denial of Service

Reputational damage

Where are we today? Controls

- Controls

Impact = Risk × Likelihood

Controls reduce the Vulnerability, the Threat, the Likelihood or the Impact.

- Physical Controls
- Technical Controls
- Procedural or Personnel Controls

A good mix of all three should give a robust system.

So where did we go wrong?

- Conquistadors' gold led to hyper-inflation.

  Is Moore's Law the conquistadors' gold of the information age?

- Do we understand the beast we've created?

Human factors

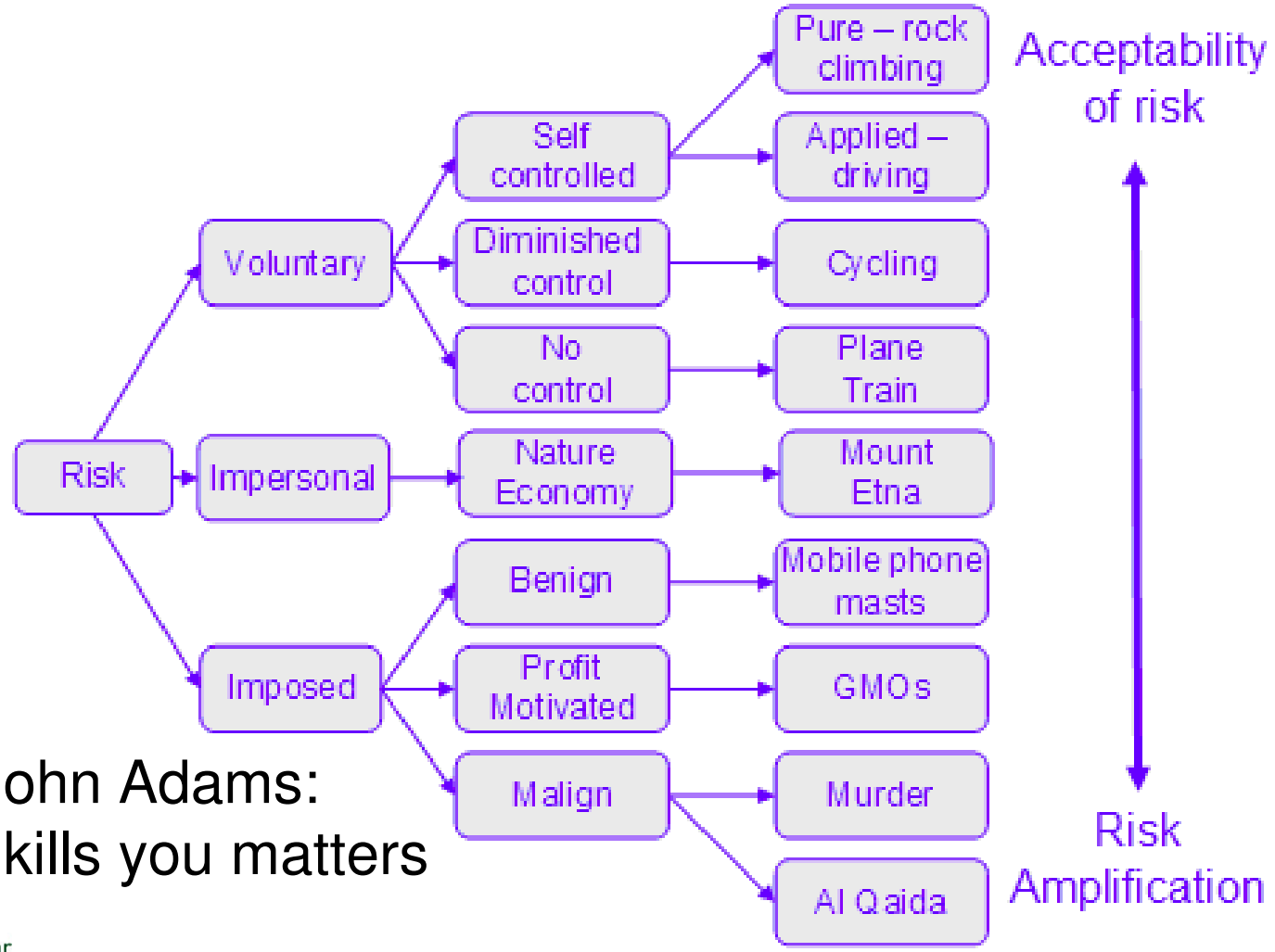
How are we at assessing risk?

- The strategies of the savannah …

… applied to the information age.

- Mental models of risk.
- The feeling and the reality of security.

What kills you matters



Prof John Adams:
What kills you matters

Personal Information – the law and the reality

- Do we understand personal information?
- DPA is perfectly clear, but is it scratching where people itch?
  - Does it match the perception of personal risk? Should it?
  - Does it provide the control people want over personal data? Should it?

Updating DPA

- Matching citizens' needs, and matching their desires.
- Greater granularity levels of personal data?
- Privacy vs Secrecy – control

Is data the pollution of the information age??

Looking for answers

So how do we make it easier?

So how do we make it easier?

Security management strategies:

- Fly-swatting
  - Always another, probably behind you.
- Checklist
  - False sense of security.
- Risk management
  - You actually have to think about it!

Golden Rules for Security Management

- Mental models are hard to change, “Flashbulb experiences”
- Understand economics – or you’ll never understand security
  - Market for lemons
  - Tragedy of the commons

Golden Rules for Security Management

- Understand the user - don't hack him off
- KISS
- Think like an attacker
- Policy must evolve. Is it still appropriate?
- So must strategy!

steria

The Chartered Institute for IT
Hertfordshire Branch

Security is hard – or is it?

Thank you for your attention