



security-assessment.com

# Social Engineering

---

Attacks against people

# About Security-Assessment.com

---

- Specialise in high quality Information Security services throughout the Asia Pacific region
- Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients
- We are committed to security research and development – Identifying & responsibly publishing vulnerabilities in public and private software
- We are an Endorsed Commonwealth Government of Australia supplier
- Sit on the Australian Government Attorney-General's Department Critical Infrastructure Project panel
- Certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs

# Agenda

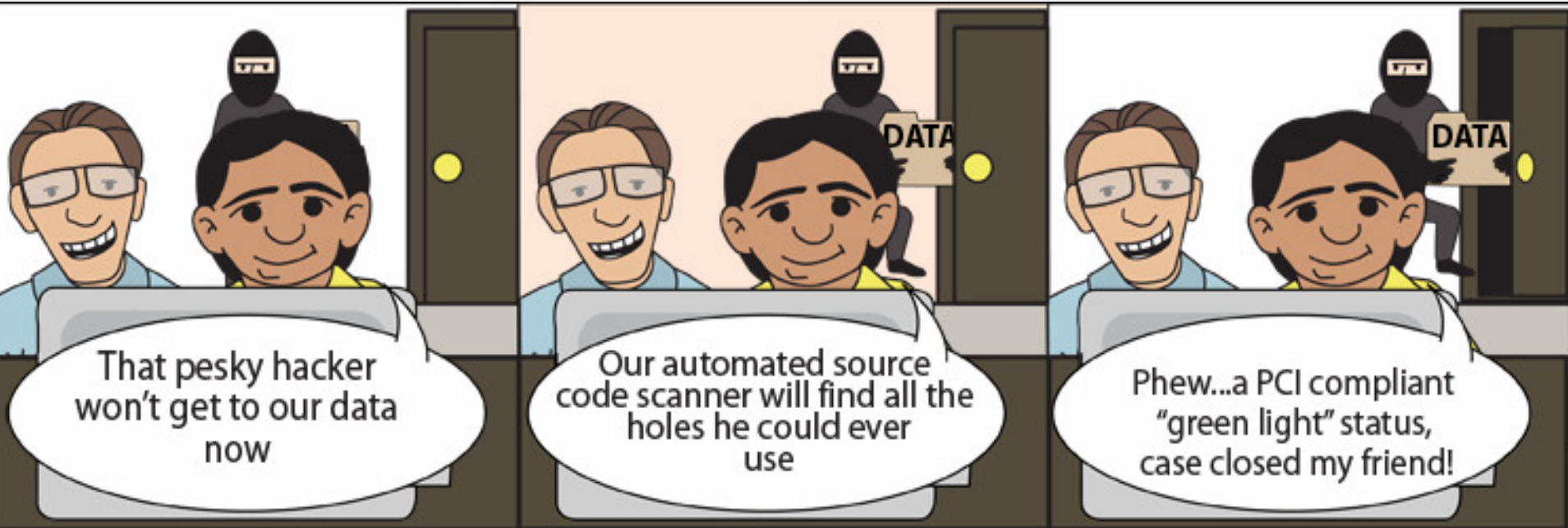
---

- What is Social Engineering
- Definitions
- From the Trenches – Real Life War Stories
- Ties to Organised Crime
- Business Risk
- Social Engineering Protection Strategies

# Social Engineering

---

Organisations can get too focussed on having all the latest technical controls but forget that people are typically one of their weakest links.



# Definitions

---

- Socialisation
- Persuasion .
- Dumpster Diving
- Phishing
- Impersonation
- Diffusion

# Why Social Engineering Works

---

- **Reciprocity Principle** - People tend to feel obliged to discharge perceived debts .
- **Authority Principle** – People tend to respond to authority figures
- **Social Proof Principle** – People tend to use people who are similar to themselves as behaviour models
- **Scarcity Principle** – People value things they perceive as scarce more than things they perceive as common
- **Consistency / Commitment Principle** – People tend to act to maintain their self image (even without conscious knowledge)

# Examples in Action

---

- Phishing – Bank Messages
- Anna Kournikova Virus
- X Box Live
- My ISP Story
- Printer Toner Theft
- Security Guards
- Nordic Bank
- HP - Boardroom Shenanigans

# The End Game

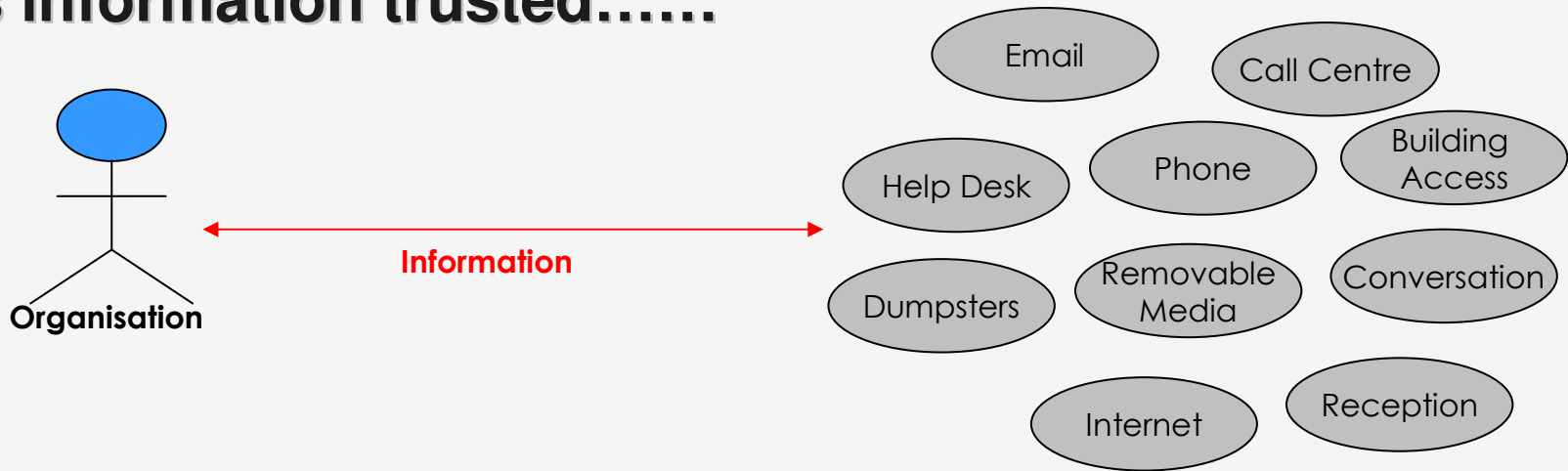
---

- Industrial Espionage
- Organised Crime
- Internal Fraud
- Stock Fraud
- Information Theft
- Identity Theft
- Intrusion and Disruption

# Assessing Threats

---

**Organisations must know how and where does / can information travel in and out of the organisation and how this information trusted.....**



**..... and ensure that the people exposed are capable of identifying a threat and adhering to policies and practices established to mitigate them.**

# Protection against Social Engineering

---

## People Need to.....

- Know what they need to do
- Be able to identify threats
- Be able to perform consistently  
- without being socially influenced to go outside defined boundaries
- Have individual accountability and sanctions for their actions

## Organisations Need to.....

- Identify all risk opportunities
- Implement strong procedures
- Provide Security Awareness Training
- Establish a Security Conscious Organisational Culture
- Tie **Individual** Responsibilities to performance
- Periodically evaluate for Human Factor Weakness

