Social Engineering

Or: The Gentle art of having others hurt themselves for your amusement

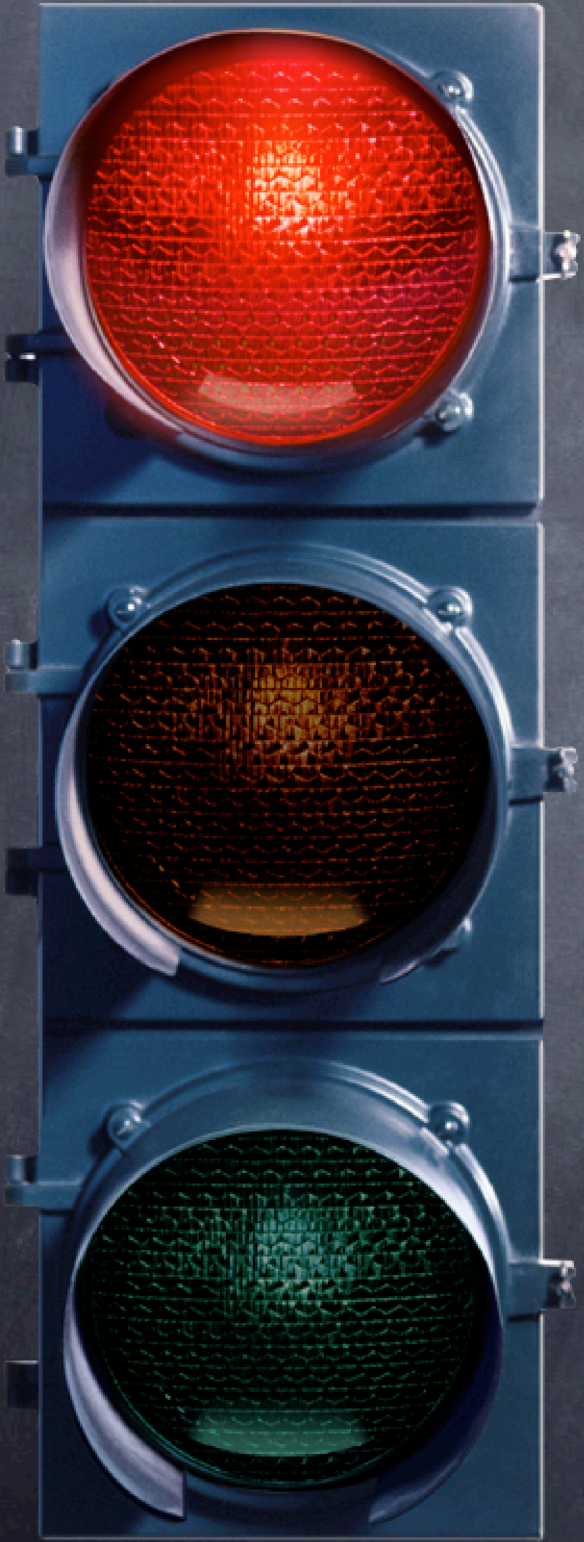
Daniel Lewkovitz M.Infotech AACS CISSP

Ruxcon email: ruxcon.20.lewko@spamgourmet.com

SECURELINK

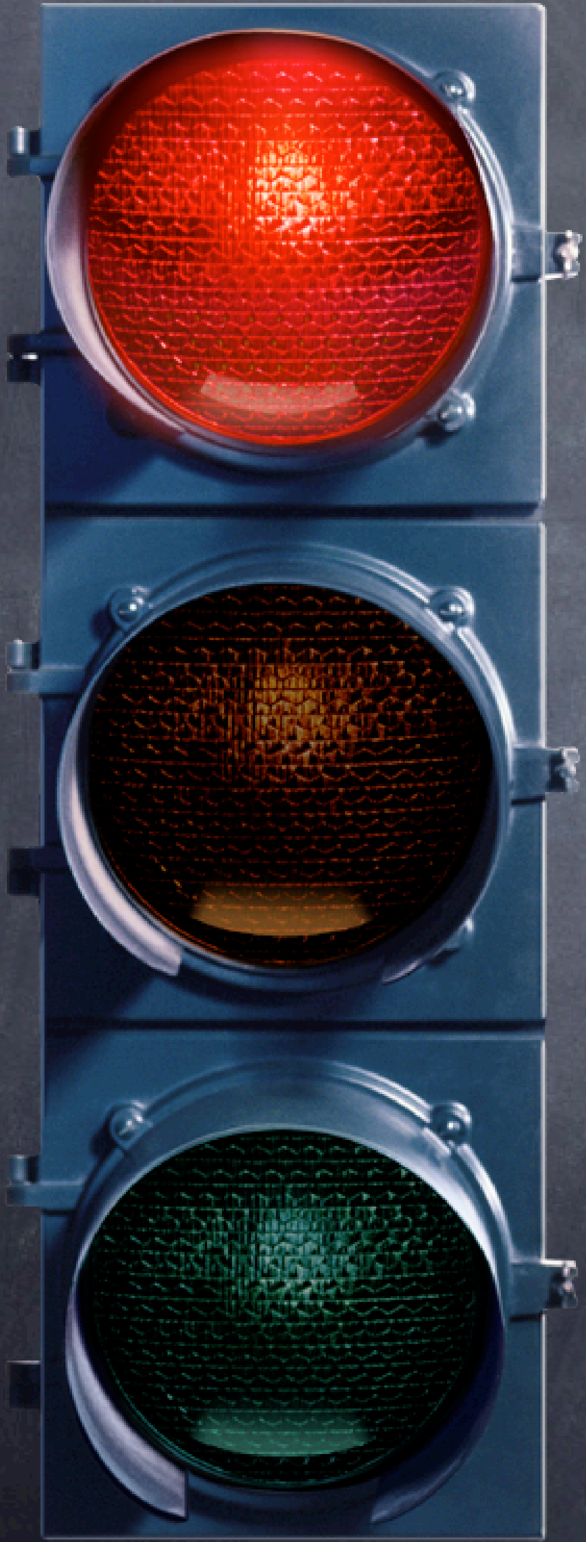
Before we begin:

- A few questions for my audience
- What is social engineering?



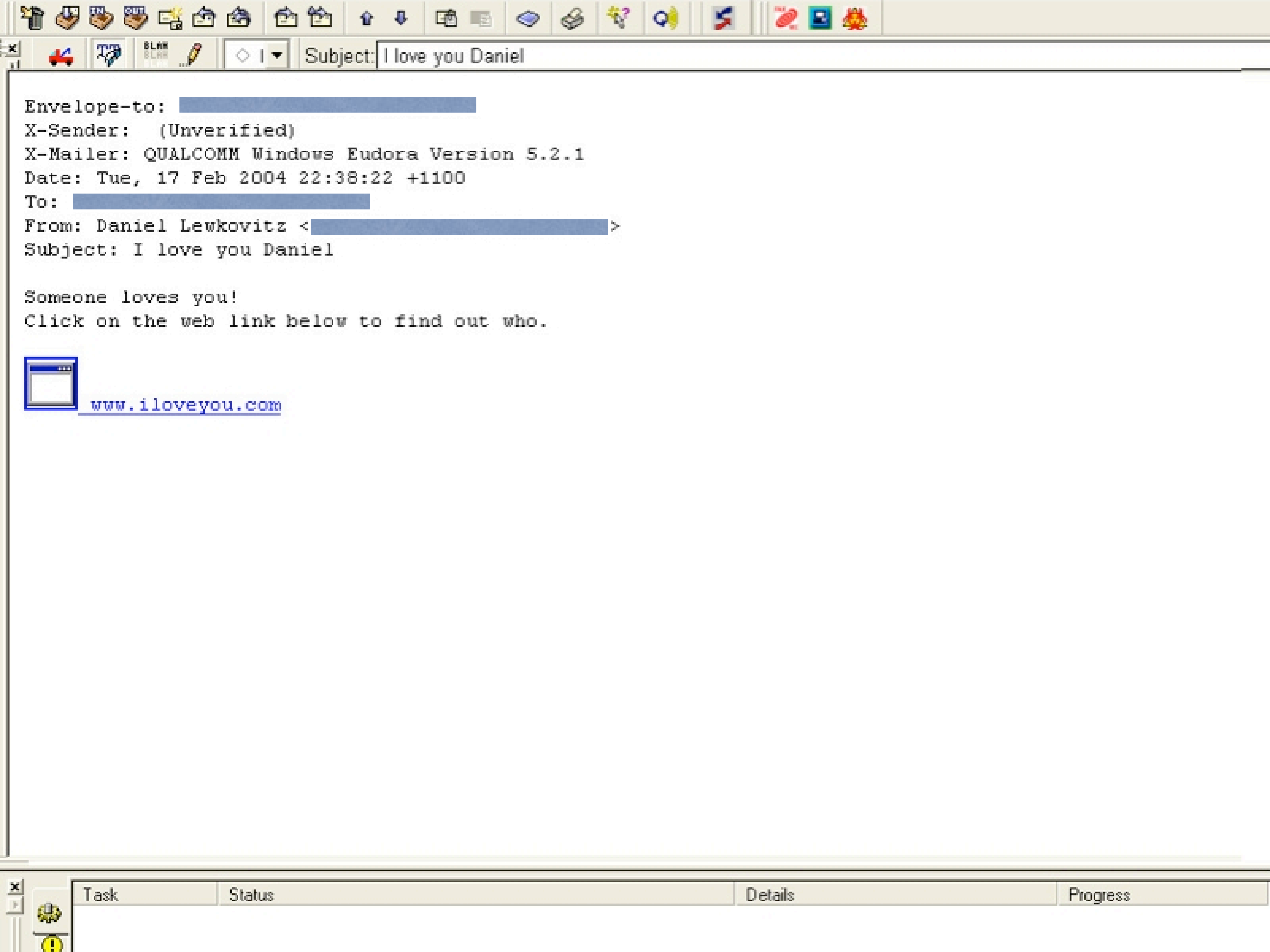
Why Technology Fails

- If you rely predominantly on technology to enforce security ***you will not be secure.***
- Airports are sadly a great example of this.
  - Metal detectors won’t detect non-metallic weapons
- Social Engineering relies on human instinct to trust others.
- Social Engineers abuse this instinct

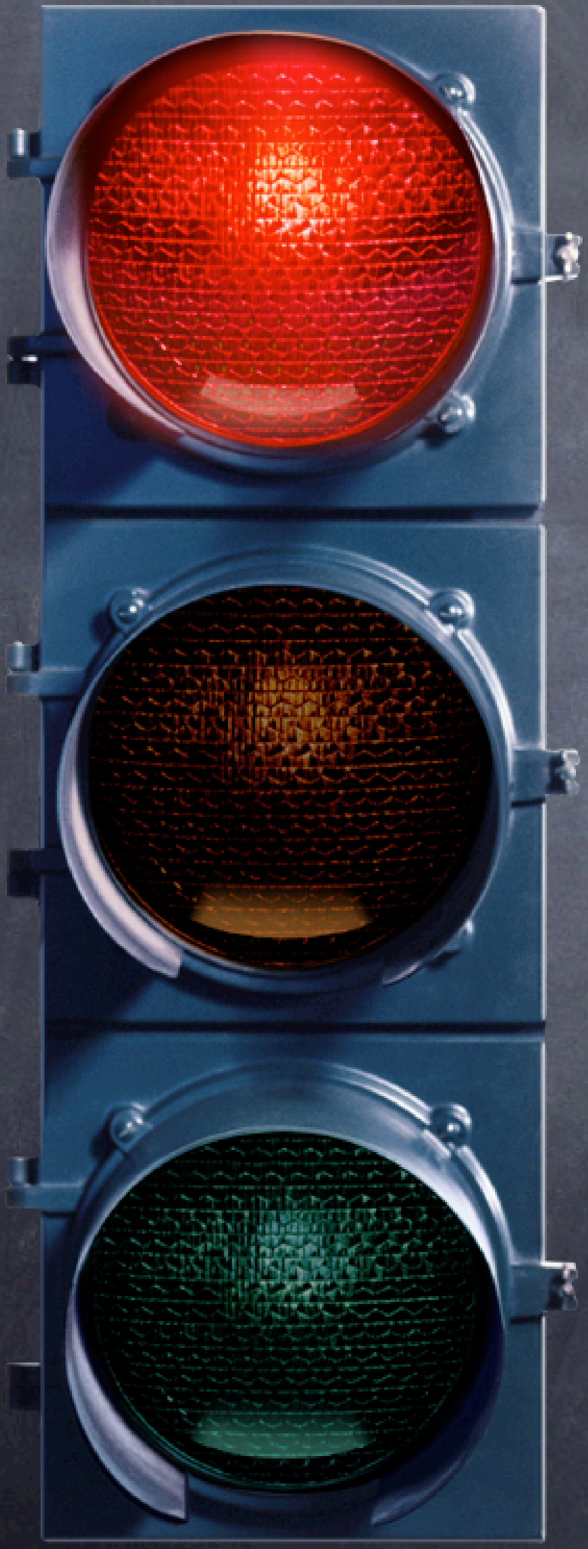


Why Technology Fails

- Virus scanners - prime example of technology to combat threat
- Inadvertent engineering attempts
  - jbdmgr.exe Hoax
  - I Love You Virus

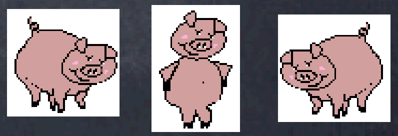


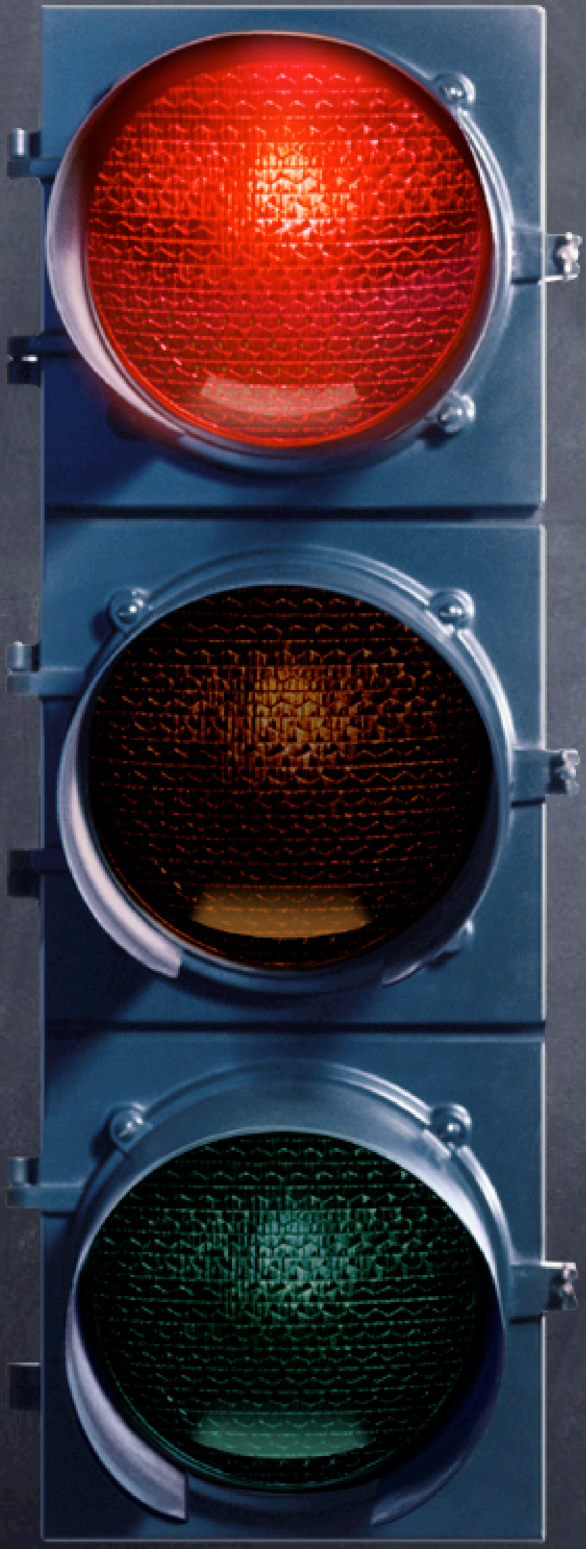
```
Envelope-to: [redacted]
X-Sender:  (Unverified)
X-Mailer: QUALCOMM Windows Eudora Version 5.2.1
Date: Tue, 17 Feb 2004 22:38:22 +1100
To: [redacted]
From: Daniel Lewkovitz <[redacted]>
Subject: I love you Daniel

Someone loves you!
Click on the web link below to find out who.

 www.iloveyou.com
```



Why Technology Fails

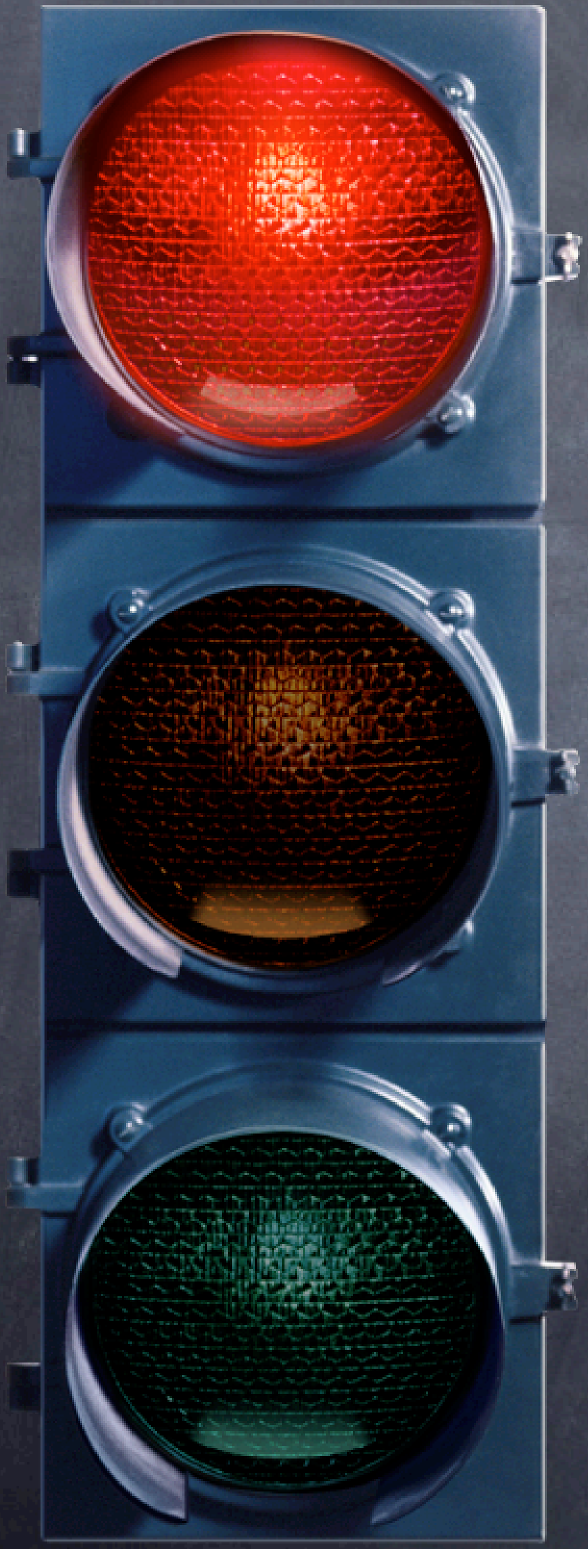
- Site specific engineering attempts
  - *Targeted attempts to elicit sensitive information or gain access to confidential resources*
- Theft of *information*
- How I disabled a $59 000 firewall...
- Your password for a pen?
- "Given the choice between dancing pigs and security, the user will choose dancing pigs every time" -- Prof. Edward Felton, Princeton University





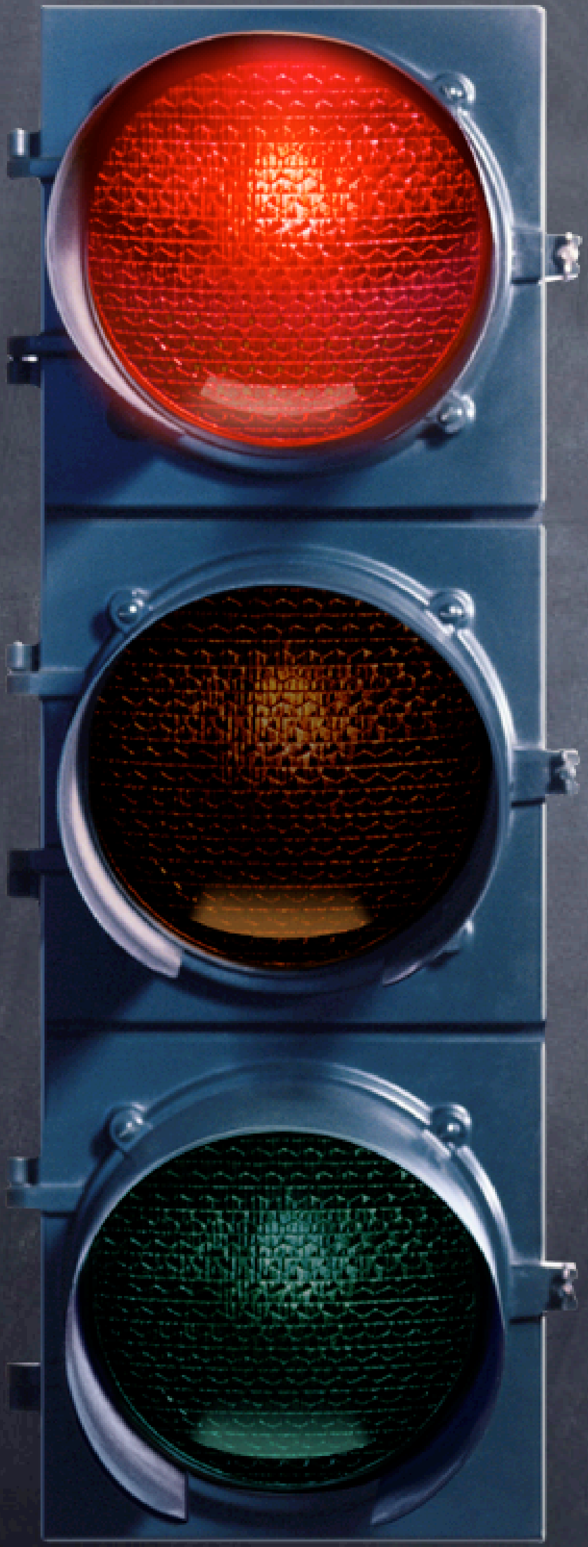
Case Study

- The following is an actual recording of an (authorised) social engineering attack on a major telecommunications provider. (Sorry - this is not available on web)
- Calls were legally recorded by company
- Sensitive information has been beeped out to protect the ‘innocent’
- Target company had several thousand employees serviced by central helpdesk
- Aim was to gain access password
- Narrative will take place on this screen



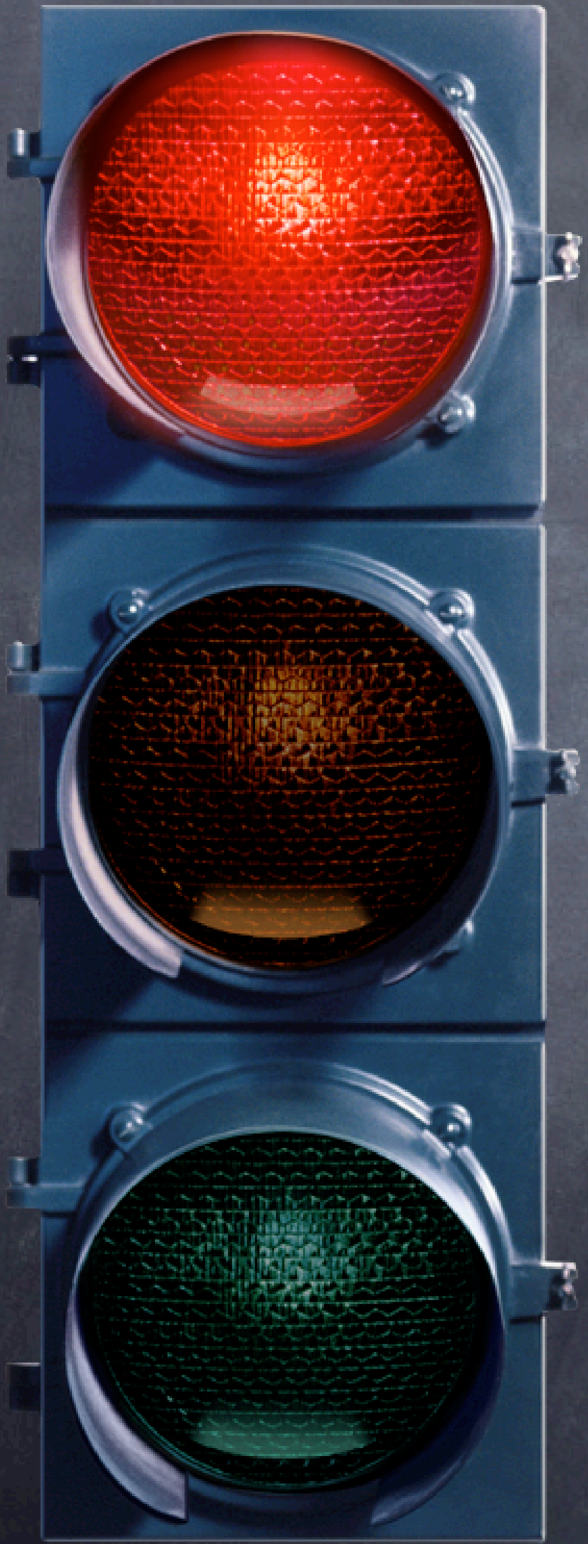
Step One

- Contacted Helpdesk with name sourced from Google Newsgroup search
- Note amount of information freely volunteered without even being solicited
- Using Citrix? Thanks for the tip!
- Vulnerable IP ranges? Thanks again!
- Friendly isn’t he?
- Problem: Need Employee Number
- Aha! The Solution. (Thanks Brad!)
- Notice answers to ‘closed questions’



Step Two

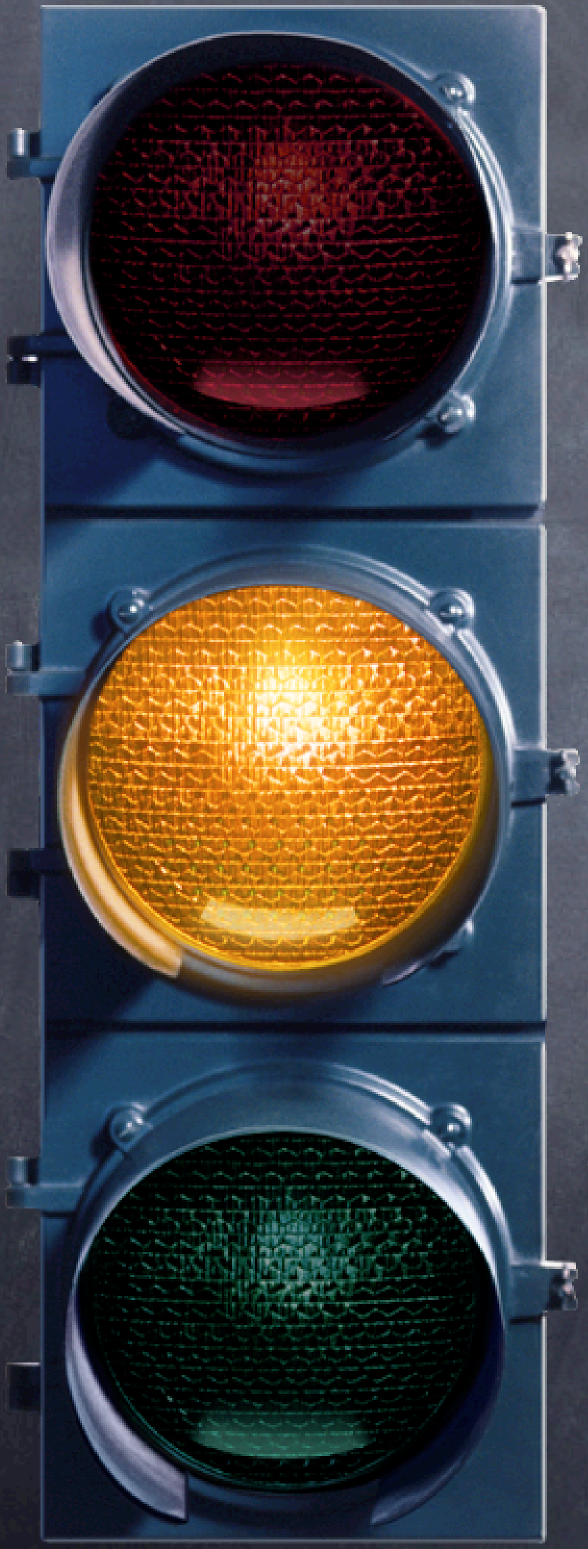
- Contacted reception via number in White Pages
- Receptionist had *no idea* this information was confidential



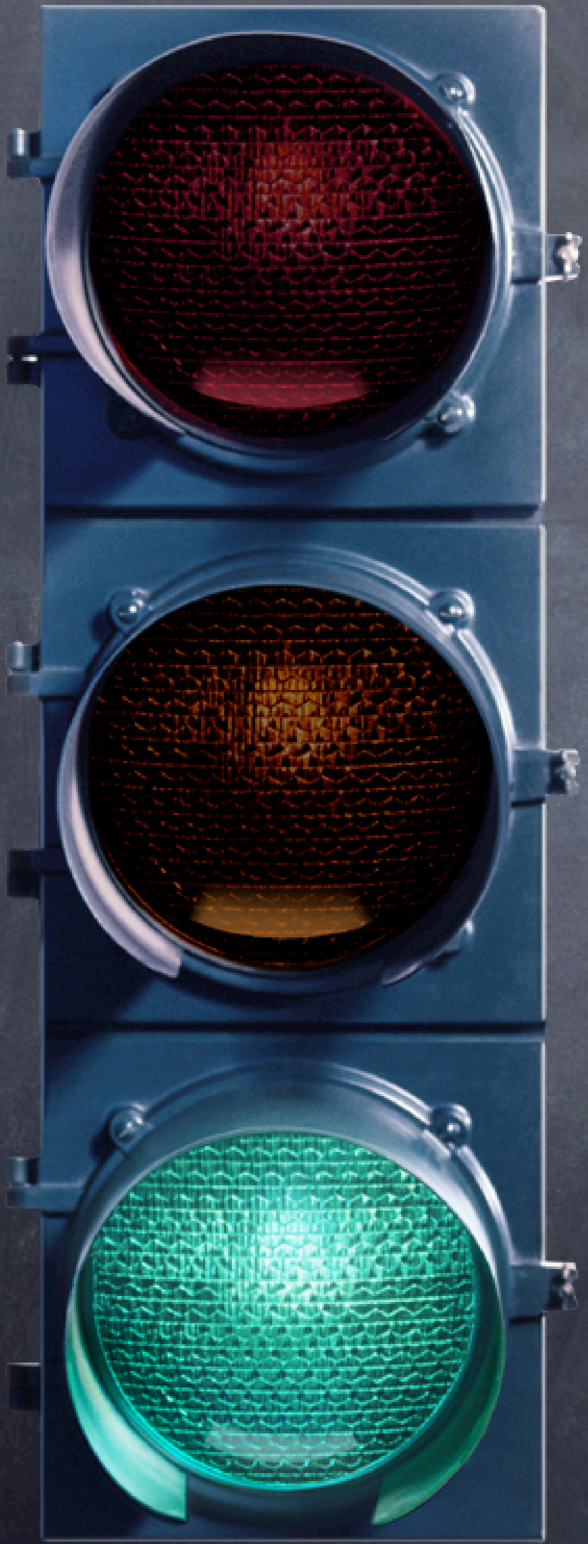
Step Three - Success

- Closed questions again!
- Question: *Would this have worked in your organisation?*

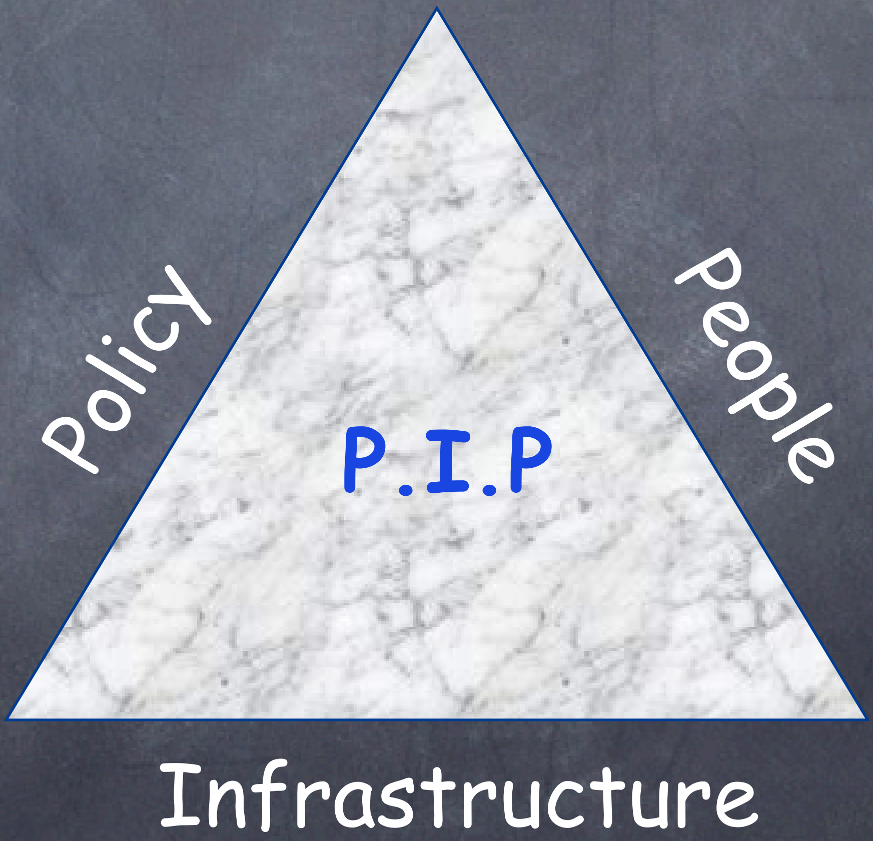
Lessons learnt



- Sophisticated identity management system and firewall complex totally defeated by password theft
- All from the comfort of my own home
- Sensitive information not identified as such:
    - Employee number
- Untrained staff forming ‘weak link’
    - Receptionist giving out information



How can we stop it?

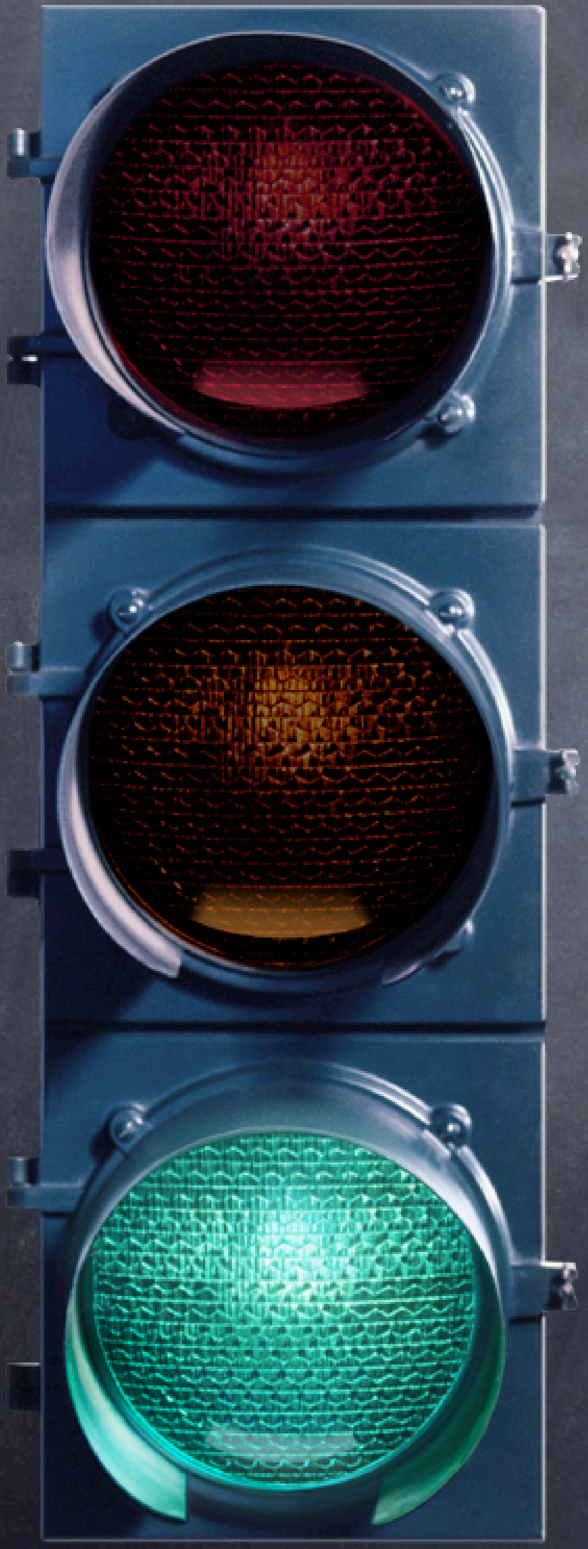


Policy

People

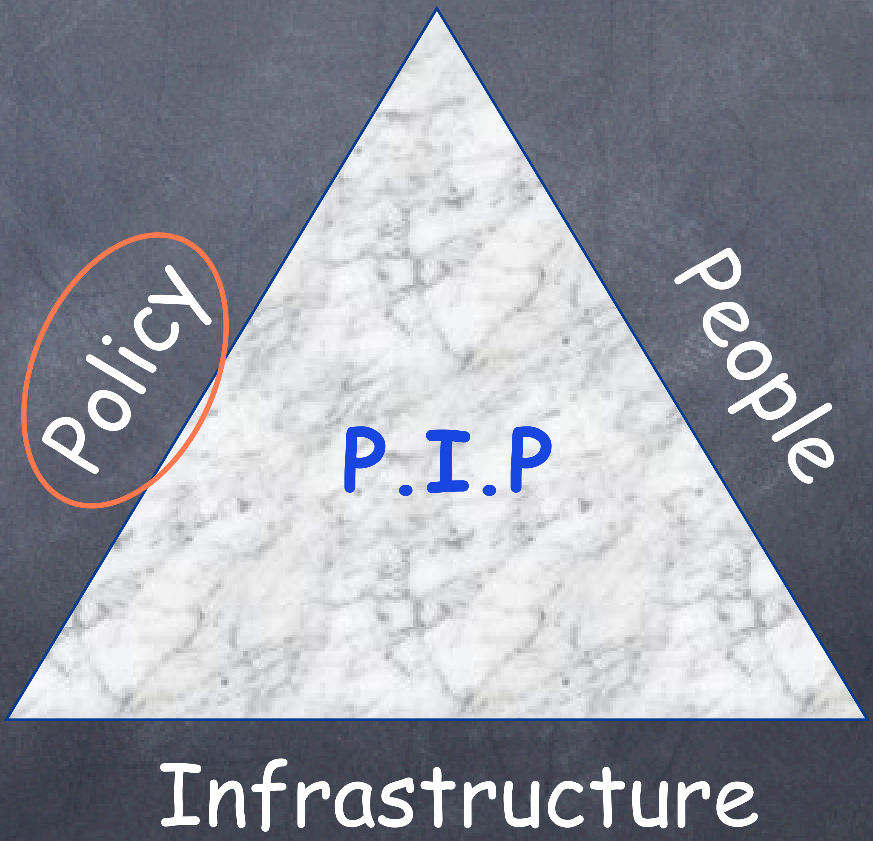
P.I.P

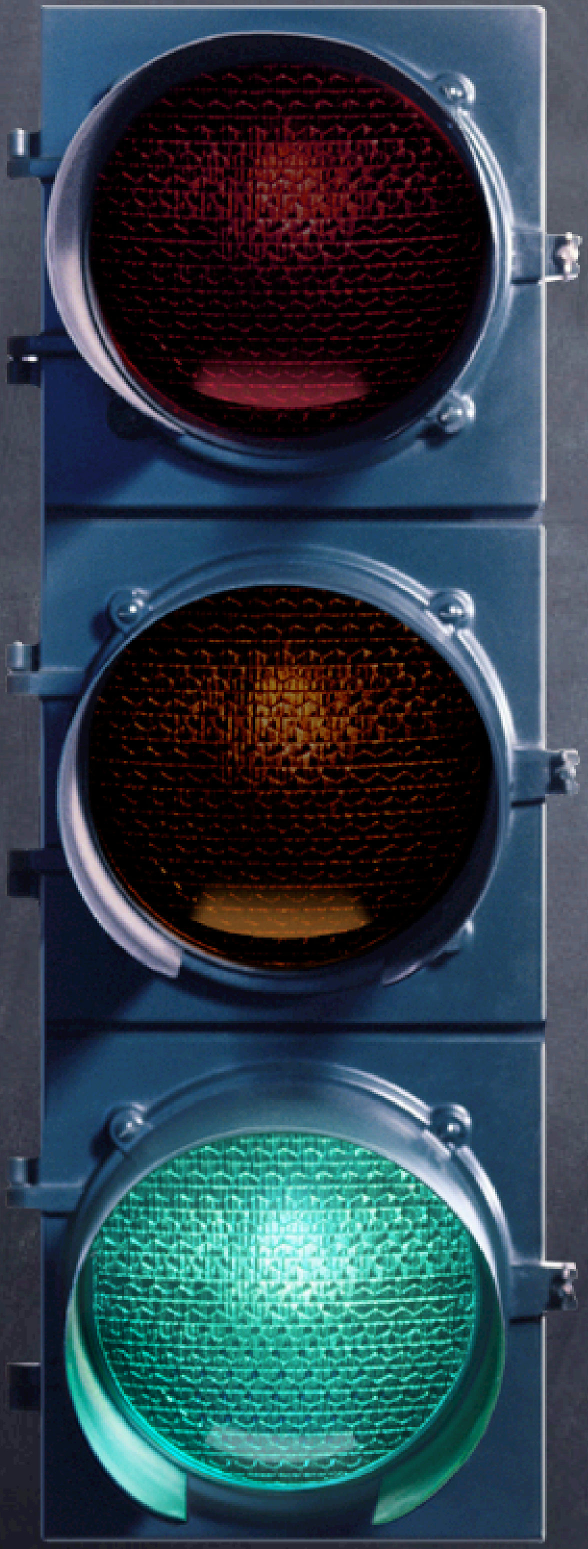
Infrastructure



How can we stop it?

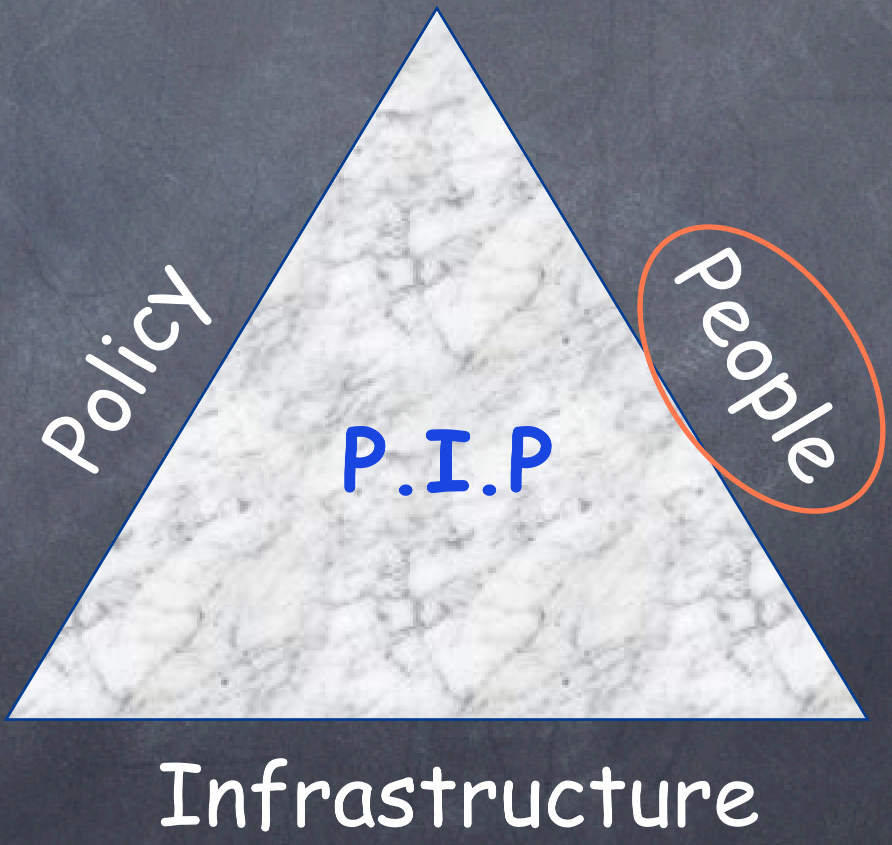
- Effective Policy
- Ensure staff awareness!

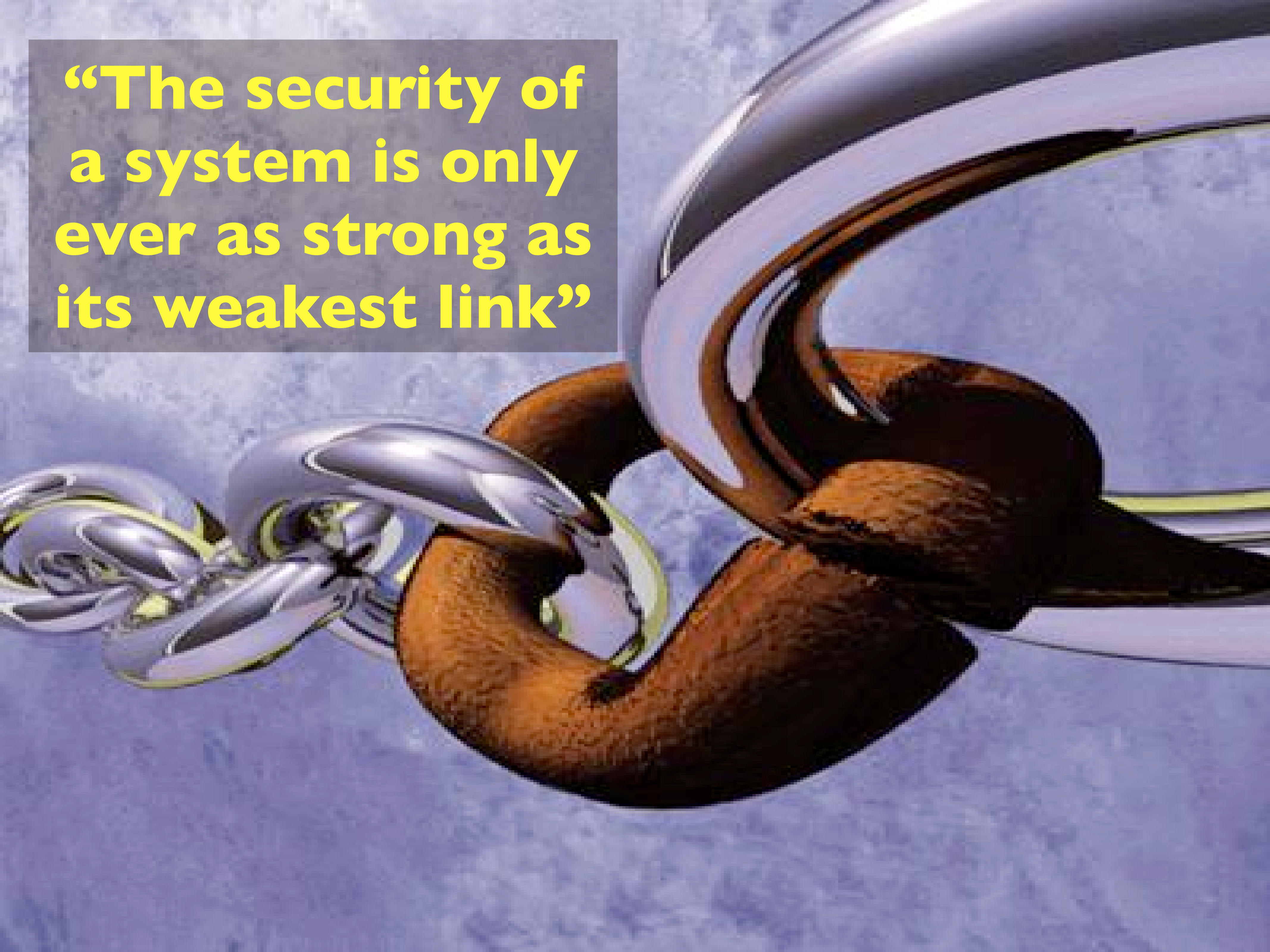




How can we stop it?

- Staff Training
- Alert staff - Stranger Danger etc.





“The security of a system is only ever as strong as its weakest link”

Why Assess Risk?

- Resources *aren't unlimited* (at least not where I have worked!) – you have to efficiently assign your time, budget, staff effort and infrastructure
- Risk assessment allows you to *prioritise* your use of *resources* in a most *efficient* manner
- Risk assessment ensures the gravest risks are duly *mitigated* rather than dropped in the "Too Hard Basket"
- Added Benefits
  - Mandatory element of AS/NZS7799
  - Helps to *quantify* risk for security business case

Why Assess Risk?

- Formal Threat/Risk Assessment methodologies are not difficult, however they are rarely ‘self-taught’ (like a lot of what we do) - If you don’t know it, learn it!
- Such knowledge and practice is common to security pros formerly of a defence or law-enforcement background.
  - Do you know any Sysadmins like this?

[redacted]

But Risk Assessment is Boring!

- Common business cases for security:
  - “If we don’t get [expensive toy] we will be hacked”
  - “If we don’t spend [χ $$$] we are out of business”
  - “I read that 93% of attacks originate from [somewhere]”

Fear Uncertainty Doubt

Fear Uncertainty Doubt

...Doesn’t work anymore

- The IT Security Manager who cried Wolf!
  - Many of us have been busily predicting the end of the world. It never happened and now management don’t believe us any more.
  - FUD is fed by media hysterics, disinformation, vendor marketing and *statistics* which aren’t always relevant to our *unique* organisations.

Hunting the Elusive Return on Security Investment

- Old attitude towards ROI: "You don't make money on security"
  - Treated like insurance - blood money
  - Many lessons learned 'the hard way' instead
  - Bad guys never tell you they failed – no *visible return*
  - Increased management skepticism post-FUD era
- Security needs to be a business enabler, not a source of pain

Hunting the Elusive Return on Security Investment

- Think about how firewall vendors now sell their products:
  - ✓ VPN device - send staff home, save money
  - ✓ bandwidth manager - increase speed, save money
  - ✓ web filtering - increase efficiency, save money
  - ✓ $$$ savings savings savings!!!

(Oh, and by the way, it's also a security device)

Training may show biggest ROI in security!

- There is no point investing $$$ in technology that can be readily bypassed by social engineering attacks
- Your adversaries *will* find the weakest link and exploit it
- Security is *everyone's* reponsibility!

Cash and Prizes

- Preventing social-engineering attacks is often called ‘impossible’ or thrown into ‘too hard basket’.
- How many of us would fall for Nigerian email scam today?
  - Why not? - Education and healthy skepticism!
- Sniffer Dog training applied to staff
  - Spot-the-intruder
  - Spot the password thief etc.

Conclusion

- Would you fall victim to attacks mentioned in today's presentation?
- Demonstrate problems to staff - they want to help!
- Train them to spot the signals and know how to respond.
- Assess your risk! Then you can treat it.
- Don't ignore it - your money spent on other security measures may be wasted.

SECURELINK

Daniel Lewkovitz M.Infotech AACS CISSP

Ruxcon email: ruxcon.20.lewko@spamgourmet.com

Certifiers of AS/NZS 7799 for SAI-Global (Standards Australia)

AS/NZS 7799 Information Security Management Audit and Consulting

AS/NZS 4360, Risk Assessment, Protective Security Manual (PSM) and ACSI33 for High Security Environments

Information Security Policy Development

Security Evaluations, Audit and Penetration Testing