

Security Fatigue: Threatening The Culture of Security

Nick Ellsmore
5-6 September 2005
APEC/OECD Security Workshop
Seoul, Korea



Outline

- Defining Security Fatigue & The Culture of Security
- The Risk Lifecycle
- Security Fatigue in Society
- Security Statistics
- Organisational Culture
- Pursuing & Achieving Cultural Change
- Risk Tolerance



“Security Fatigue”

- Definition
 - Desensitisation and risk tolerance within a community or organisation leading to an increased risk exposure
- Drivers
 - Information Overload
 - Warnings without actualisation
 - Over-shooting risk assessments
 - Information in the public domain inconsistent with the day to day experience of the community



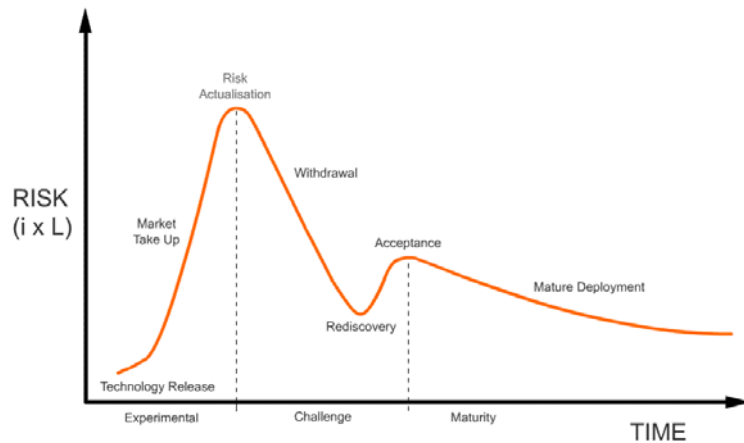
“Culture of Security”

- OECD "Guidelines for the Security of Information Systems and Networks", July 2002
 - Goal of a “Culture of Security”
- United Nations General Assembly Resolution A/RES/57/239 for “Creation of a Global Culture of Cyber Security”, December 2002
- Recognised by the Council of Ministers of the APEC forum and by the Council of the European Union





SIFT® Risk Lifecycle



Security & Risk

- Information security is similar to other areas of human “security”
 - Health / “bio-security” / disease
 - Lies, Damn Lies and Statistics
- Lack of understanding in the general community
- Easy to stir fear and uncertainty
- Wide application / impact
- Media coverage is often based on exceptional occurrences





Safe Sex

- Professor Adrian Mindel, Director of the Sexually Transmitted Infection Research Centre
 - “While substantial declines in the incidence of both bacterial and viral STIs were observed throughout the 1980s and early 1990s, **new diagnoses of STIs have risen continually since 1995.**”
 - “These statistics indicate that **people have become complacent about safe sex and are increasingly engaging in high-risk behaviours** such as multiple and concurrent partnerships and inconsistent condom use.”



Road Deaths

- Professor Peter Brooks, Executive Dean of the Faculty of Health Sciences at the University of Queensland
 - In 2003, 1,634 people died on Australian roads and many thousands were injured
 - World Health Organisation has estimated that by 2020, road trauma will have moved **from ninth to third place** on the list of disorders causing most death and disability around the world
 - Internationally, approximately 3000 people die every day on the roads
- Cause of complacency: “We drive so often and nothing happens”



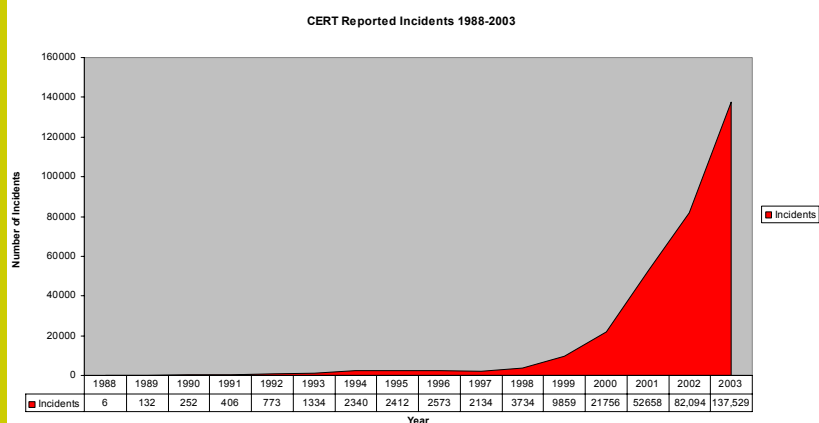


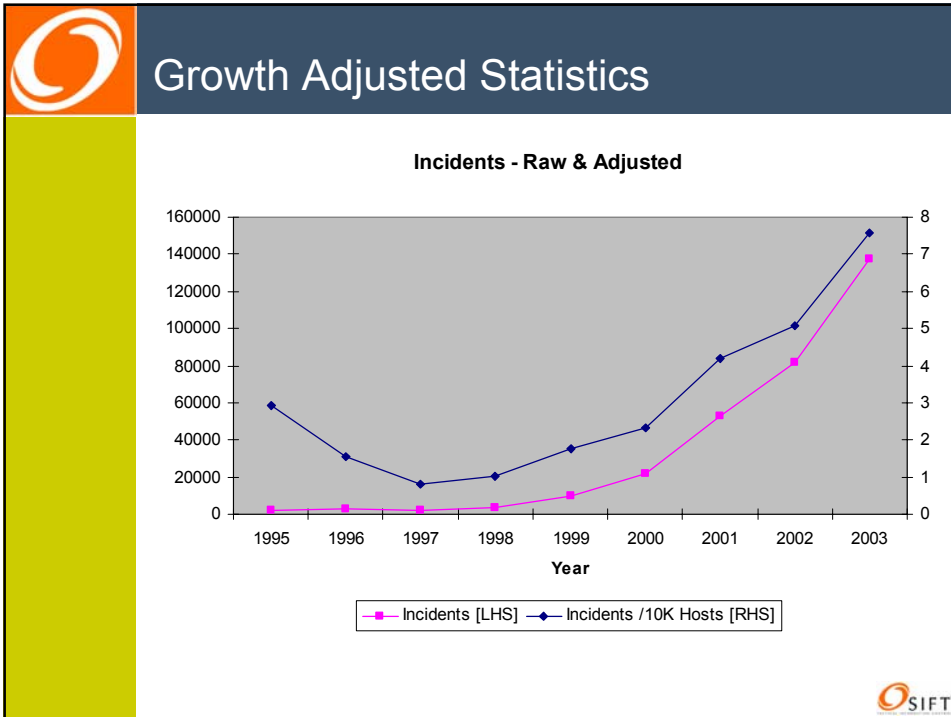
How Much Do We Know?

- In believing we understand the type, scope and scale of the issues involved, we introduce complacency
- A lack of security incidents does not demonstrate successful security management!
- How realistic are the statistics we are using?
Example: CERT Statistics vs Adjusted Statistics



CERT Statistics – The Scary Graph





-
- Growth Adjusted Statistics**
- Less than eight (8) reported incidents per 10,000 hosts.
 - Raw Growth: 57-fold increase 1995 to 2003
 - Adjusted Growth: 2.6-fold increase same period
 - Need to focus surveys and control more variables
- SIFT



Organisational Culture

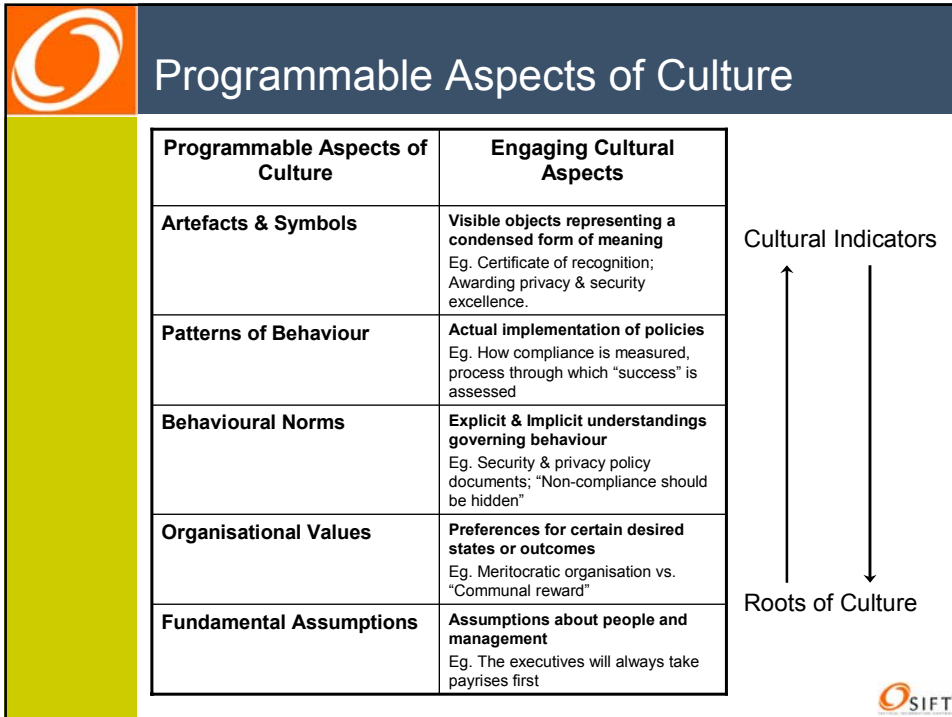
- Culture can be defined as:
 - That complex whole which includes knowledge, beliefs, law, morals, customs and habits acquired as society members
 - Shared by almost all members
 - Passed on from older to younger
 - Influences an individual's perception and behaviour
- Organisations can also have “subcultures” and cultural conflict.
- It is through this culture that security fatigue and doubt propagate



Basis of Organisational Culture

- Within an organisation, culture can include:
 - “The way we do things around here”
 - “Shared meanings” and/or
 - “The collective programming of the mind”
- This may include:
 - Shared Assumptions / Beliefs
 - Company Policy
 - Personnel Practices
 - Work Flow and Work Loads
 - Management and Supervisory Styles
- Influencing the organisation's culture is key to ensuring new initiatives are taken seriously.





Affecting Organisational Change

- Managers or Organisational “Champions” can have a positive influence on organisational culture by:
 - being a "role model" for the staff
 - rewarding appropriate behaviour
 - communicating to staff what behaviour is desired in as many ways as possible
 - providing training to highlight the activities that the manager is trying to encourage.
- Policies & procedures that are not enforced will entrench a culture of non-compliance.

SIFT



Conclusions

- People are often willing to accept risks that are not theirs to accept
 - Risk exposure often reaches far wider than the individual accepting the risk
- Fear is not a compelling driver of action over the long-term
- The statistics around information security are necessary but not sufficient to build a compelling case
- Focused campaigns at improving information security understanding and take-up are necessary
- Cultural recognition of the importance of information security is necessary to avoid security fatigue



Questions

Nick Ellsmore

E: nick.ellsmore@sift.com.au

W: www.sift.com.au

P: +61 2 9236 7276

