Beyond hackers, viruses and worms

Protecting critical activities from cybercrime and cyber-terrorism
The Infosec theatre of war

General vulnerabilities

- External attacks
- Attack and response dynamics

Internal headaches

- Unaware users,
- Malicious insiders,
- Weak identity management
- Back doors,
- Logical bombs,
- Undocumented functions

... and more...

Virus, worm, trojan horse writers,
Script kiddies & other hackers,
Zombies in DDOS mode,
Hactivists and spoof sites
Organized crime
Cyber-warriors and cyber-terrorists
... and more...

Information workshop at OECD
Paris, October 2004
Types of attack

Physical attacks

Syntactic attacks

Semantic attacks

Corrupt data in “trusted” systems

Make computers perform unexpected functions

Information workshop at OECD
Paris, October 2004
Protection against insider threats

Stage 1: Policies, monitoring and compliance

Stage 2: Building protection features into systems

Stage 3: Operational administration and monitoring

Stage 4: Investigations and digital forensics
Malicious insider

Queensland (AUS) Sunshine Coast, April 2001

Disgruntled employee hacks into computerised sewage control system. Released one million litres of raw sewage.

Motivation

Opportunity

Knowledge

Found guilty on 46 counts of computer hacking

Sentenced to two years in jail

What if he and others like him had been suborned by terrorists or a foreign government?
Stage 1: Policies and compliance

Appropriate use of ICT resources
Authentication and identity management
Access rights “need to know” or unrestricted
Irresponsibility, impropriety and fraud
Computer crime and audit strategies
Monitoring
Worker* references and credentials

* employee, temporary staff, contractors, consultants, interns, visitors, maintenance personnel, cleaners, etc.
Stage 2: Building features

System design safeguards and controls
Back doors and logical bombs
Partition of data in support of “need to know”
Authentication systems
Storage safeguards
Controls - qui custodiat custodies?
Review and validation
(no Easter Eggs, no undocumented functionality, no unknown superusers, etc)
Stage 3: Operational matters

Identity management and MACs
Superuser rights management
Data rights (C, U, R)
Disclosures and social engineering
Monitoring tools, privacy and ethics
Controls – qui custodiat custodies?

*MAC = moves, additions and changes
CUR = create, update, read only*
Investigation and digital forensics

- Determining point of access and containment
- Setting up traps
- Evidence preservation and custody chain
- Evidence analysis and forensic tools
- Collaboration between HR, Internal Audit and I.T.
Organization’s metabolic rate

Ability to recruit and train
Career progress criteria
Background vetting/clearances
Flexible remuneration
Fast procurement processes
Budgetary room to breathe
Culture of openness

Assumption: many critical infrastructures are managed with a slow metabolic rate
From cybercrime to cyberterrorism

Same skills, same tools, different intent

Achieve media coverage
Impact economic systems
Destabilise civilian life
Asymmetric warfare against law enforcement
Hurt trust in governments’ ability to protect citizens
Use “successes” to gain more support for their cause

Guns
Explosives
Chemical weapons
Bacteriological weapons

AND/OR
Planning for defensive success

Are traditional infrastructure operations, audits, etc still good enough

What can we learn from the “bad guys”

How do we learn how bad guys think and operate

How do we incorporate this culture into our defences