SERT

Security Emergency Response Team

Alan W. Coulter
Director
Prentice Centre
The University of Queensland
Qld 4072
A.Coulter@cc.uq.edu.au

SERT

Overview

* Why do we need SERT?
* What is SERT?
* SERT's role
* SERT's relationships
* SERT activities
* SERT contacts

SERI

Connectivity

USA	1,000,000
Germany	100,000
UK	88,000
Australia	82,000

SERT

Why Do We Need SERT?

* Success of CERT Coordination Centre in USA
* AARNet is large (>80,000 hosts)
* Need security coordination locally
* Reduce costs to AARNet members
* Aid to small sites
* Establish and maintain trusted relationships

What is SERT?

* Security Emergency Response Team
* Trusted Centre of Security Expertise
* Analysis of Security Incidents
* Response to Security Incidents
  → help sites
  → recommend a defence
* Dissemenation of Security Information
* Education and Security Tools

SERT

What Will SERT Do For Me?

* Provide help on computer security and liaison
* Recommend action for known vulnerabilities
* Central source of security information
* Raise security awareness
* Preserve confidentiality and privacy
* Comply with relevant Laws

What Won't SERT Do For Me?

❋ Can't fix your security problems

➡ will provide assistance

➡ will provide pointers

❋ Will not take disciplinary action on your behalf

How Was SERT Formed?

* Cooperative venture - UQ, QUT, GU
* Funding locally first half 1993
* Funding support from other universities second half 1993
* Function recognised by AVCC - request for tender

SERT

SERT's Relationships

* 24 Hour trusted contact for security
* Trusted contacts with its constituents
* Law enforcement agencies
* FIRST - Forum of Incident Response and Security Teams
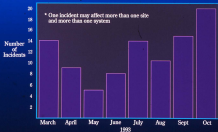* Information Security Research Centre

SERT's Relationships

* CERT Coordination Centre (USA)
* Joint Network Team (UK)
* DFN - CERT (Germany)
* CERT - NL (Netherlands)

What Has SERT Done So Far?

* Operational since 8 March 1993
* Handled > 100 incidents
* Large incident involving a coordinated tftp attack
* Emergency after hours site notification
  - wuarchive
  - gopher
  - sendmail

SERT

What Has SERT Done So Far?

* Issued ten advisories
* Megapatch
* Technical papers on security issues
* Local ftp archive site
* Assistance to the AFP

SERT

Why Should I Register With SERT?

* Receive security information
* Assistance with security incidents
* Part of a security conscious community
* Contact if a vulnerability or attack is determined

SERT

How Do I Contact SERT?

* Phone: (07) 365 4417 – SERT staff answer during Qld. business hours.
  AEST = GMT + 10:00.
  On call after hours for emergencies

* Fax: (07) 365 4477

* Email: sert@sert.edu.au