

Building Incident Management Capabilities

Robert Lowe



- Started in 1993
- Not for profit, member funded
- Based at the University of Queensland

- Has performed the National CERT role for Australia
- Assistance with CSIRT establishment



- **Funding**
 - Workable business model?
- **Governance**
- **Mission**
 - Objectives
 - Services

Services



AusCERT
Australian Computer Emergency Response Team

Reactive Services



- + Alerts and Warnings
- + Incident Handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
- + Vulnerability Handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination
- + Artifact Handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination

Proactive Services



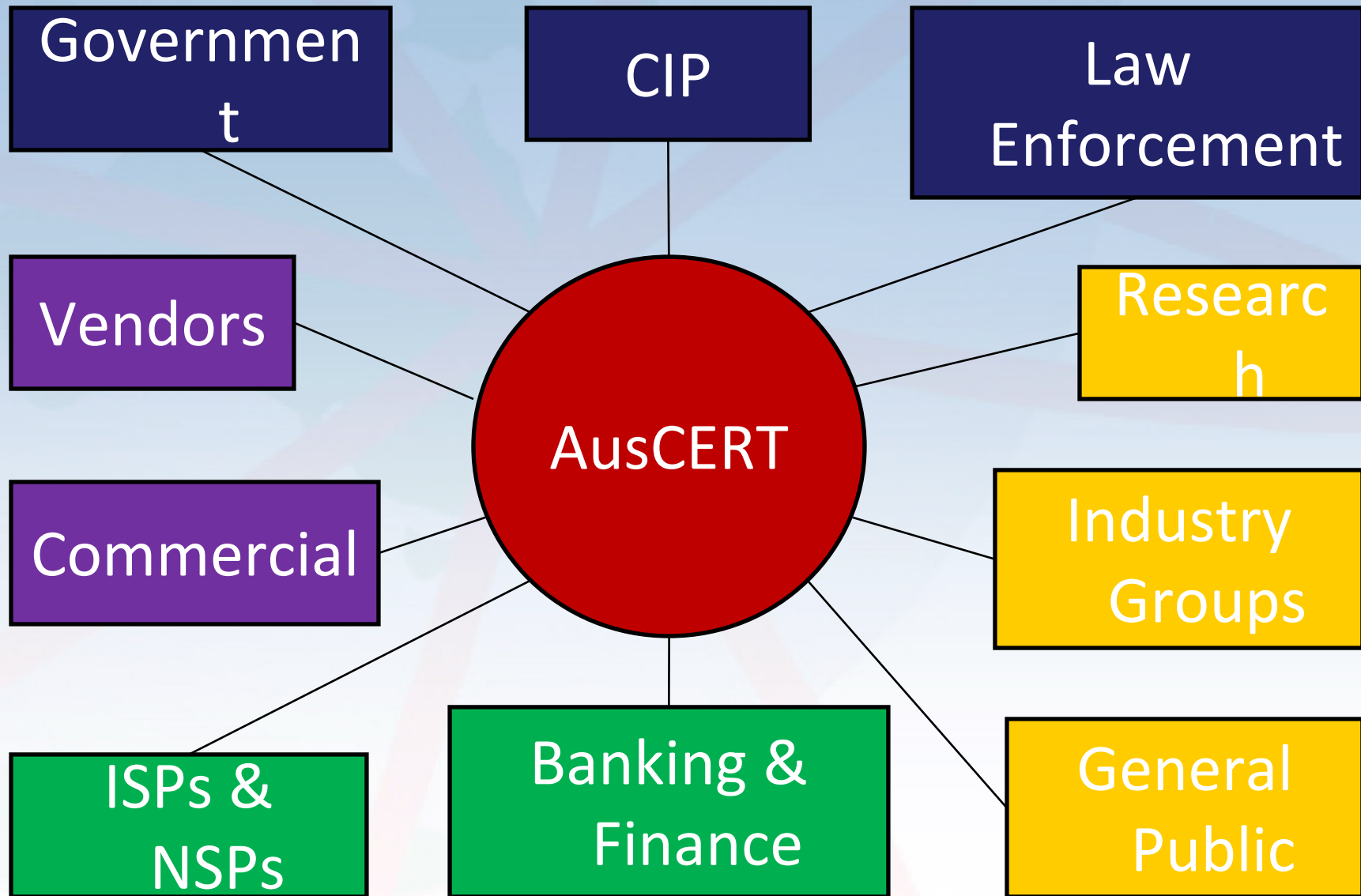
- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Source: Carnegie Mellon University/Software Engineering Institute
<http://www.sei.cmu.edu/pub/documents/03.reports/pdf/03hb002.pdf>



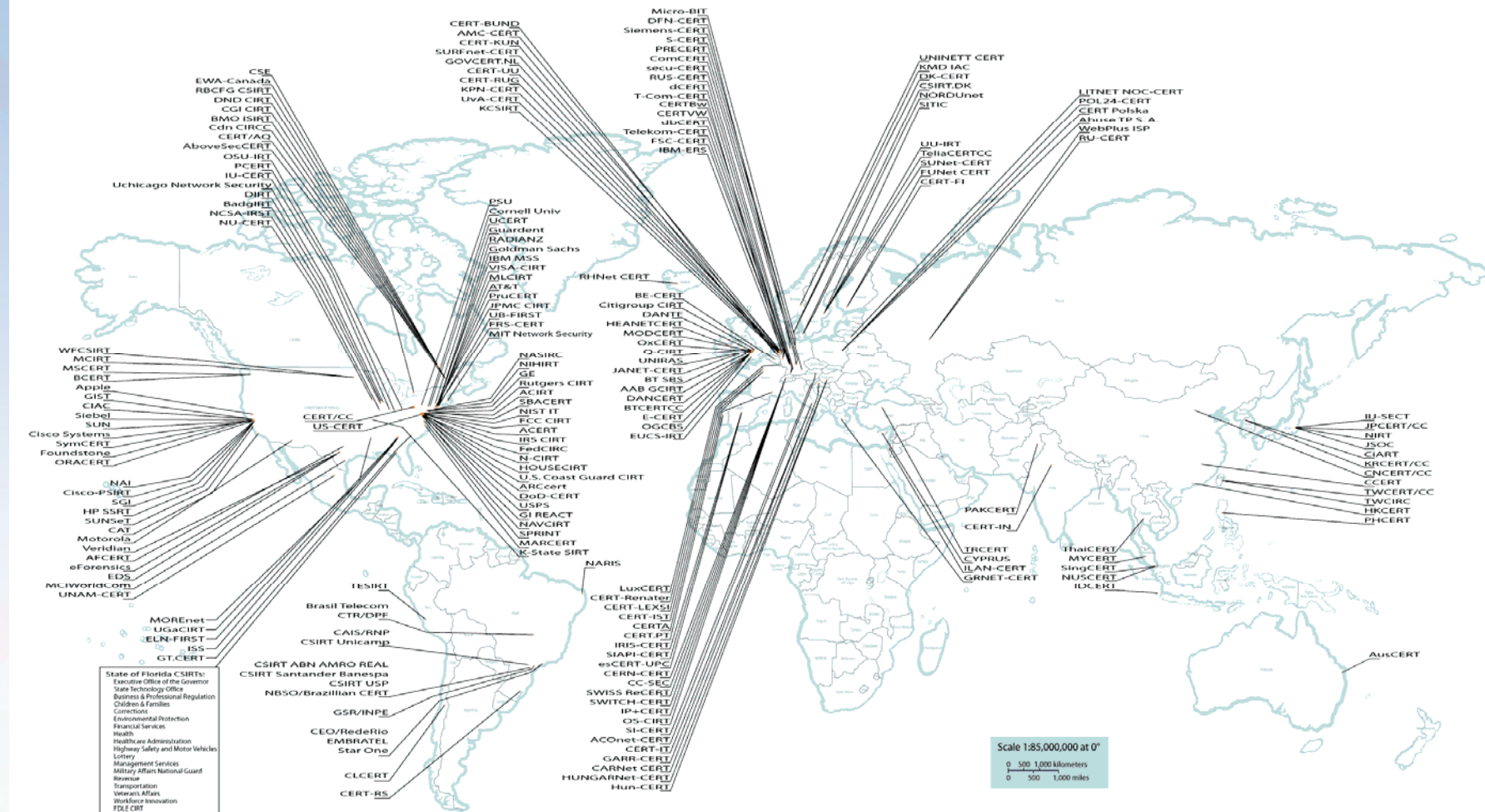
Worldwide relationships



AusCERT
Australian Computer Emergency Response Team

Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.

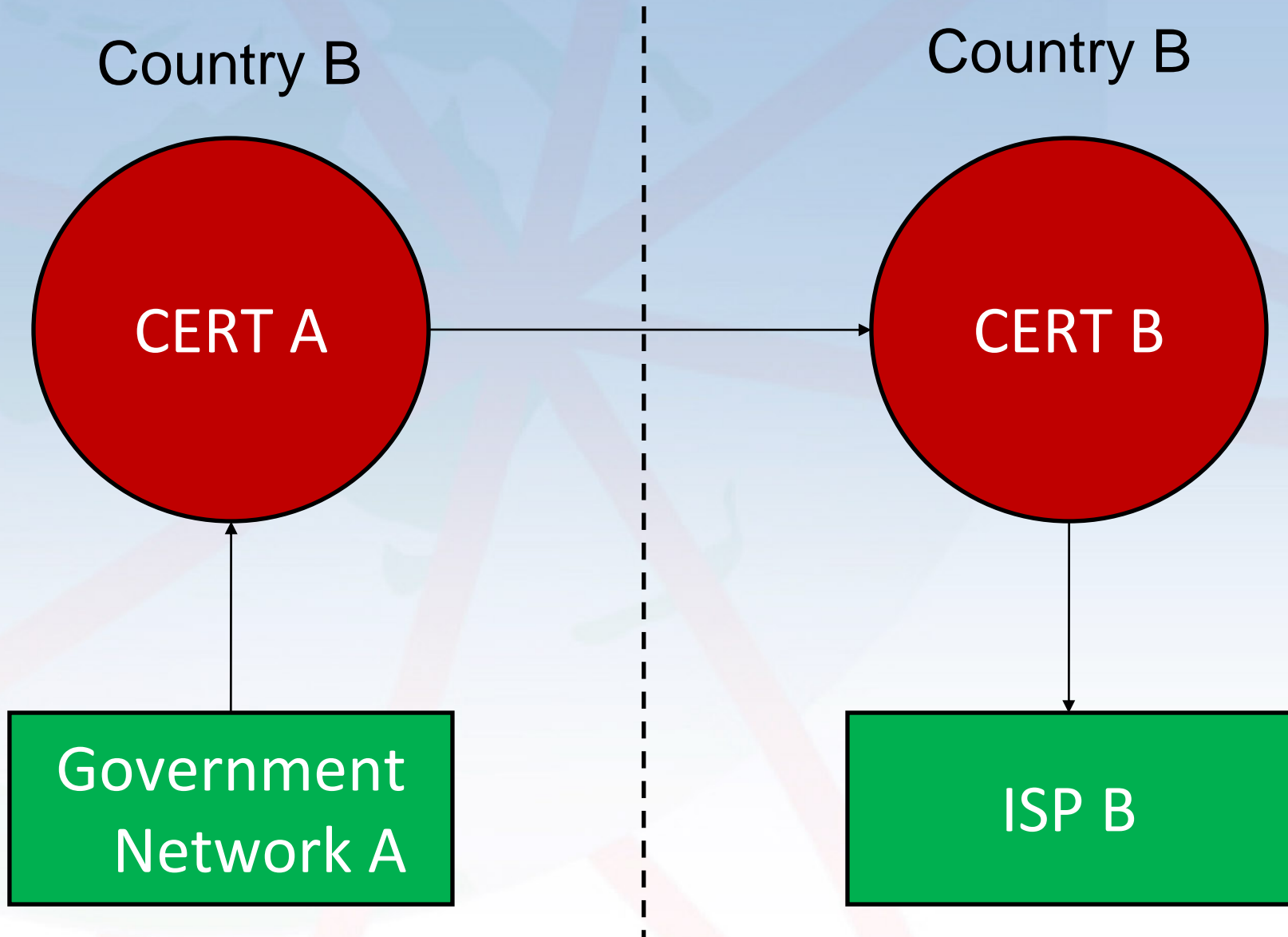


Source: CERT Coordination Center <http://www.cert.org/csirt/csirt-map.html>

International cooperation



AusCERT
Australian Computer Emergency Response Team

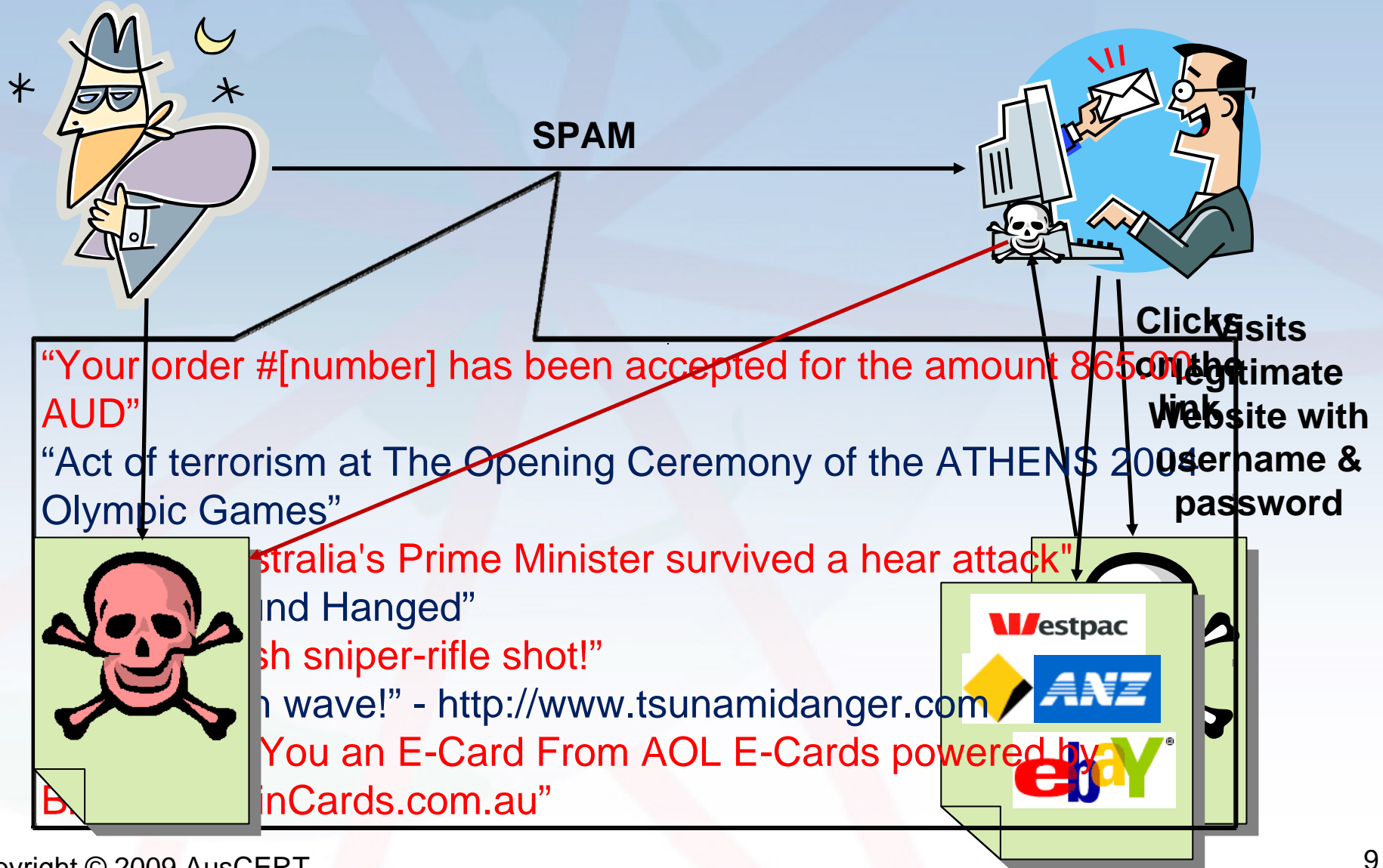




- **Trust**

- Information sharing
 - Assistance
 - Often person, rather than organisational
-
- Actively maintained
 - Mutually beneficial
 - Often informal

Credential theft





- AKA: Trojans, hijacking malware, password stealers
- Not just “the bank’s problem”

“The last 12 months have been the worst I’ve seen for credential stealing malware.” (Q2, 2009)

- But what gets all the media attention?
- Conficker



- **About 1 in 7 people are using a compromised system**
- 46% believed that it is not possible for an attacker to see or modify data from a HTTPS session
- 38% believe they can rely on AV/anti-spyware to alert them to malware infections

