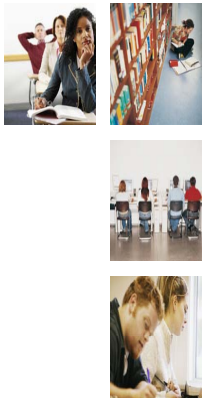


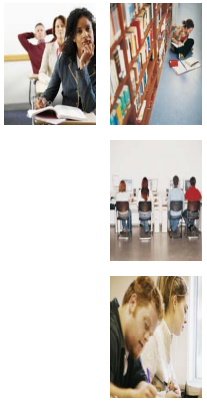
WARPs and CSIRTs:
Thoughts on synergy

Andrew Cormack

Chief Security Adviser, UKERNA

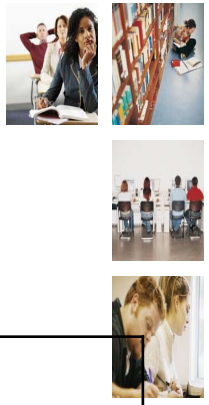
A.Cormack@ukerna.ac.uk

WARNING



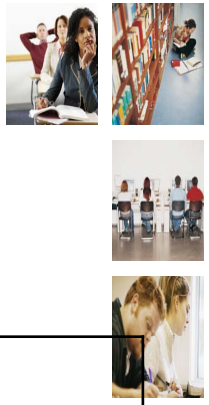
- These are very much thoughts in progress
- My ideas will develop during the day!
- Please point out errors/misunderstandings/etc.
- either now or afterwards

Comparing Cultures & Relationships



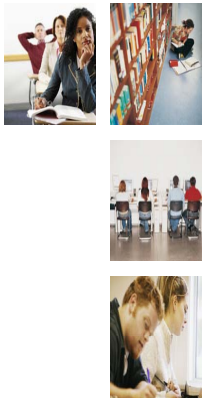
	CSIRTs	WARPs
Customers	(Large) constituency	Small community
Linked by	Common policy	Common interest
Contacts	Nominated	Volunteer
Perceived status	“Expert”	First among equals, self-help
Main priorities	Incident response; incident prevention	Incident prevention; empowerment

Comparing Tasks & Methods

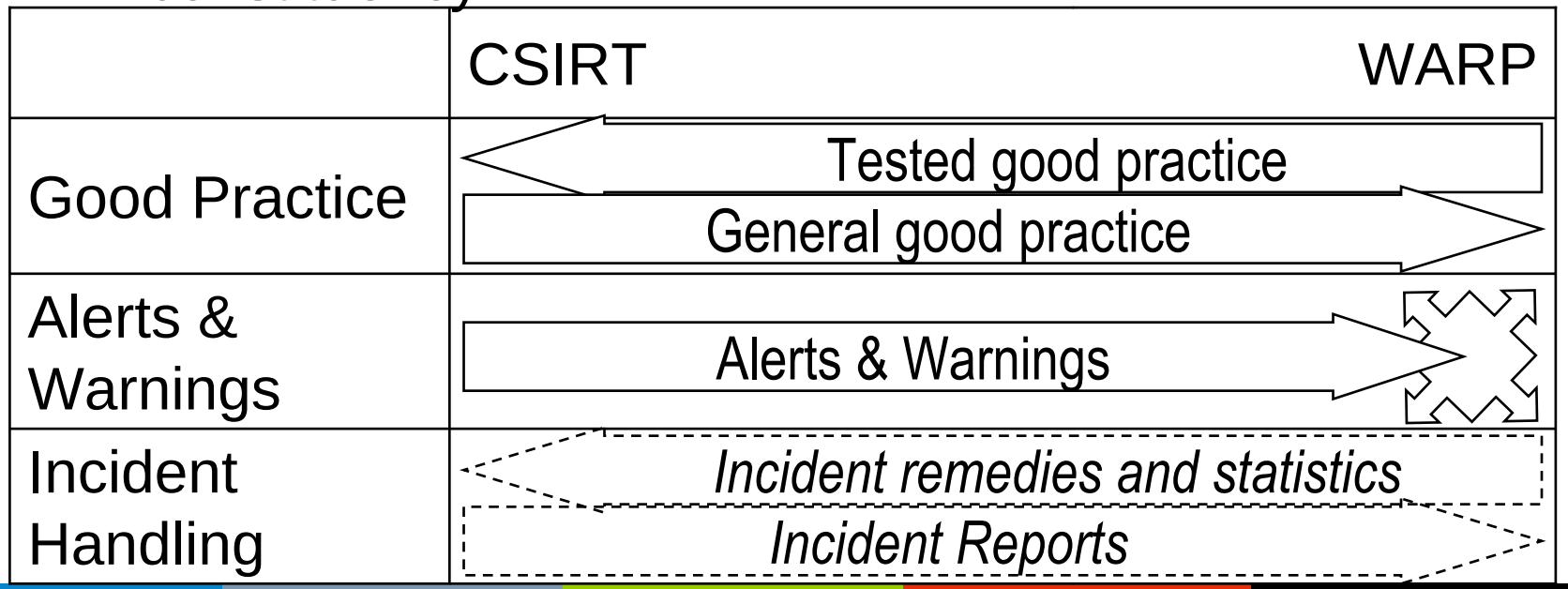


	CSIRTs	WARPs
Good practice	Identify and disseminate	Share
Alerts and warnings	Disseminate (may create); collect from constituency	Select, tailor & disseminate; share among community
Incident Handling	Resolve incidents within and between constituencies	Exchange lessons learned within community

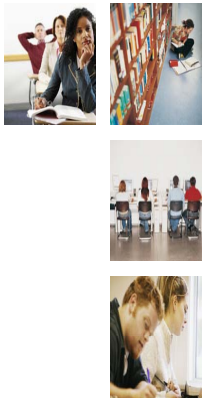
Information Flows



- Lots of opportunities for useful relationships
  - Need to make sure these benefit both sides
  - May be possible even if WARP is not in CSIRT constituency



Development



- Closer WARP/CSIRT partnerships
  - As trust develops and usefulness becomes clear
- ? Cluster of WARPs with a parent CSIRT
  - Each concentrates on what it does best
  - Should give best relationship with members
- ? Large WARP might become a CSIRT
  - Change of emphasis and priorities
  - Needs community agreement, as more info is exposed
  - Will change relationship with community