Mobile Malware Incident Exercise

- On 23 Dec 2012 two Oil companies from your country separately contact you about a mobile malware attack they are experiencing – looking for your help
- They have done some initial analysis and found that it is an Android worm spreading via MMS and Bluetooth.
- The malware also drops a windows executable on the memory card which. if run, will infect any other phone connected to the infected PC
- They have done some research and believe this to be a targeted attack.
- No AV vendor detects the malware.
- The malware sends the following message:
  - "Download the official Energy Industry app from www.energyConferences.com and stay up to date on all Oil and Gas industry conferences and events"
- The Registrar for the Domain is in your country
- The IP for the domain is on bullet proof hosting in Eastern Europe
- The Whois details are obviously faked.
- The malware also appears to download a commercial Android spyware onto the phone, allowing it to record calls, send files etc.

- Both companies need help knowing how to:
- **Contain** this threat – i.e. Stop it getting any worse
- **Eradicate** the threat - remove all traces of it
- **Recover** – i.e. Get back into production and monitor the situation
- They would also like to determine the initial point of infection if at all possible.