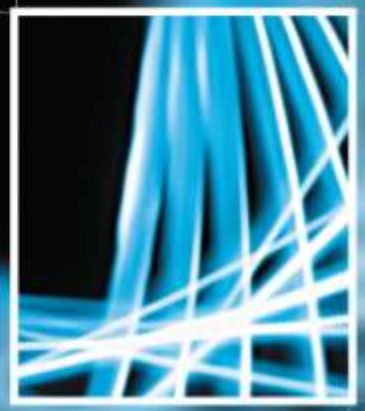

UK Networks & Security
An Overview

Dr Andrew Powell, ENISA Workshops on CERTs in Europe, 29 May 2008

CPNI
Centre for the Protection of National Infrastructure

Objectives

- The structure of your public communication networks
- The threat landscape these networks face
- The key players in Network Information Security that you have identified as crucial for your national response plan
- Cooperation initiatives with these key players and how you get them involved
- The layout of your response plans to prepare your country for cyber attacks and threats
- An example where these plans were put to a test

CPNI
Centre for the Protection of National Infrastructure

UK Communications Networks: A Market View

- Highly diverse, competitive market
- Many different operators in the voice and data markets
- BT and Cable & Wireless are the largest providers in terms of overall market share for fixed line communications, but …
- Data and voice services unbundled to promote equality of access to customers for all operators

CPNI
Centre for the Protection of National Infrastructure

UK Communications Networks: Technological View

- Networks are in transition between separate voice and data networks to unified networks using Internet protocols
- Backbone networks are optical fibre with end to end fibre for many businesses and cable customers but with a lot of access networks still being copper for voice and broadband
- Synchronous Digital Hierarchy (SDH) is still the dominant optical transmission technology using Time Division Multiplexing (TDM)

CPNI
Centre for the Protection of National Infrastructure

UK Communications Networks: Technological View (II)

- Asynchronous Transfer Mode (ATM) and Frame Relay are still in widespread use over SDH, but …
- IP based networks are starting to run over Wave Division Multiplexing (WDM) networks that use Ethernet (or Provider Backbone Bridging Traffic Engineering, PBB-TE) to provide the data link layer
- SDH may be incorporated for network resilience
- Multi Protocol Label Switching (MPLS) using IP routing to establish the switches is common in data networks

CPNI
Centre for the Protection of National Infrastructure

UK Communications Networks: Types of Network

- Internet data (and derived voice) networks
- Private business data (and derived voice) circuits
- Broadcast networks
- Telephony networks
  - Fixed
  - Mobile
- Emergency response networks
  - Satellite
  - Radio

CPNI
Centre for the Protection of National Infrastructure

UK Communications Networks: Resilience

- No simple network diagram for the UK
- Resilience supported by:
  - A large number of international cable routes
  - Satellite
  - Diversity in technology
  - Diversity in network and service provision
  - Redundancy in architecture by large national operators

CPNI
Centre for the Protection of National Infrastructure

UK Communications Networks: Threat

- Theft of metals and equipment (criminals)
- Denial of service (protestors/criminals)
- Interception (nation states/criminals)
- Traffic degradation/modification (nation states/criminals)
- Iconic sites in the sector (terrorists)

CPNI
Centre for the Protection of National Infrastructure

Response: Who does what

- UK separates security from resilience
- Resilience
  - The National Emergency Alerting for Telecommunications (NEAT) scheme run by the operators under the direction of a government/business group, the Electronic Communications Resilience and Response Group (EC-RRG)
- Security
  - GovCERTUK for UK government networks
  - CSIRTUK for co-ordinating incidents affecting private sector organisations
  - Incidence response teams from individual operators
  - UK police for crime reports and criminal investigation and the Serious and Organised Crime Agency (SOCA) eCrime directorate
  - There is strong engagement with international partners in Europe (European Government CSIRTs group (EGC) and the TERENA's Task Force for CSIRTs (TF-CSIRT))

CPNI
Centre for the Protection of National Infrastructure

Engagement with Responders

- Emphasis on government/business partnership
  - EC-RRG for resilience
  - UK Network Security Information Exchange (NSIE) for security
  - Relationships between CSIRTUK, GovCERT and response teams from individual operators
- Preparation and response to national crises supported by the Civil Contingencies Act 2004
- No regulatory/statutory framework for security (unless a crime has been committed), but …
- Work is underway on a minimum security standard for the communications sector based on a subset of ISO27011

CPNI
Centre for the Protection of National Infrastructure

Engagement with Responders

- Emphasis on government/business partnership
  - EC-RRG for resilience
  - UK Network Security Information Exchange (NSIE) for security
  - Relationships between CSIRTUK, GovCERT and response teams from individual operators
- Preparation and response to national crises supported by the Civil Contingencies Act 2004
- No regulatory/statutory framework for security (unless a crime has been committed), but …
- Work is underway on a minimum security standard for the communications sector based on a subset of ISO27011

CPNI
Centre for the Protection of National Infrastructure

Preparing for Attacks

- There is policy that covers the UK government approach to protecting its national infrastructure
- There is a national information assurance strategy led by the Cabinet Office
- The Centre for the Protection of National Infrastructure (CPNI) has the remit of working with businesses to reduce the vulnerability of the UK's national infrastructure
- CPNI does provide security advice on all aspects of protective security including publications, many of which are available on http://www.cpni.gov.uk
- CPNI supports the Business Enterprise and Regulatory Reform department (BERR) in identifying the UK's critical communications infrastructure with operators and providing tailored protective security advice
- Details of mitigation for vulnerabilities are published by CSIRTUK

CPNI
Centre for the Protection of National Infrastructure

Attacks on the UK's Communications Infrastructure

- There has to date not been any attacks on the infrastructure which have caused a national loss of service of any aspect of communications
- Hazards (such as fires) have caused local outages
- Targeted denial of service attacks on data networks are common
- Attacks on data services such as email are common (targeted or otherwise)
- Attacks on communications infrastructure are known, for example:
  - Domain Name System denial of service attacks
  - Border Gateway Protocol (BGP) attacks including hijacking of address space
  - Fraudulently offering services
  - Router compromise for spamming
- CSIRTUK has been the mechanism for dealing with security incidents and the NEAT process is the mechanism for addressing resilience incidents

CPNI
Centre for the Protection of National Infrastructure

Contact Details

Dr Andrew Powell

Tel: +44-207-233-8181

Email: andrewp@cpni.gsi.gov.uk

Web: http://www.cpni.gov.uk

CPNI
Centre for the Protection of National Infrastructure