Information Sharing and Trust in Business Continuity

David Sutton

BANG

25th September 2013

tacit.tel
consulting

Agenda

- Introduction
- How it all began . . . and developed
- Information Exchanges
- Trust
- NEISAS

British Computer Society

- Certificate in Information Security Management Principles (CISMP)
  - Information Security Management Principles (Second edition) 978-1-78017-175-3
- Practitioner Certificate in Information Risk Management (PCIRM)
- Practitioner Certificate in Business Continuity Management (PCBCM)

- CESG Information Assurance Professionalism Programme (IAPP)

Other work areas

European Public Private Partnership for Resilience (EP3R)

Distance Learning MSc in Information Security

Training accreditation

CISMP, PCIRM and PCBCM training courses

How it all began . . .

- 6th December 2001
  - Kick-off meeting sponsored by Oftel & Cabinet Office
- Early 2002
  - Telecoms Industry Emergency Planning Forum (TI-EPF) formed Oftel, Cabinet Office, DTI, Fixed & Mobile Network Operators
- 29th March 2004
  - Manchester tunnel fire
  - Agreement for inter-operator exercises
- January 2005
  - First inter-operator exercise
- July 2005
  - London bombings
  - Buncefield oil terminal fires

. . . and developed

- 2006
  - Name change to EC-RRG
- 2007
  - Part of Exercise Long Shadow
  - Severe flooding – Severn & Thames
- 2009
  - Ilford cable tunnel breach
  - Granted access to Airwave Sharers List
  - Exercise White Noise
- 2010
  - Paddington telephone exchange flooding

Electronic Communications Resilience & Response Group

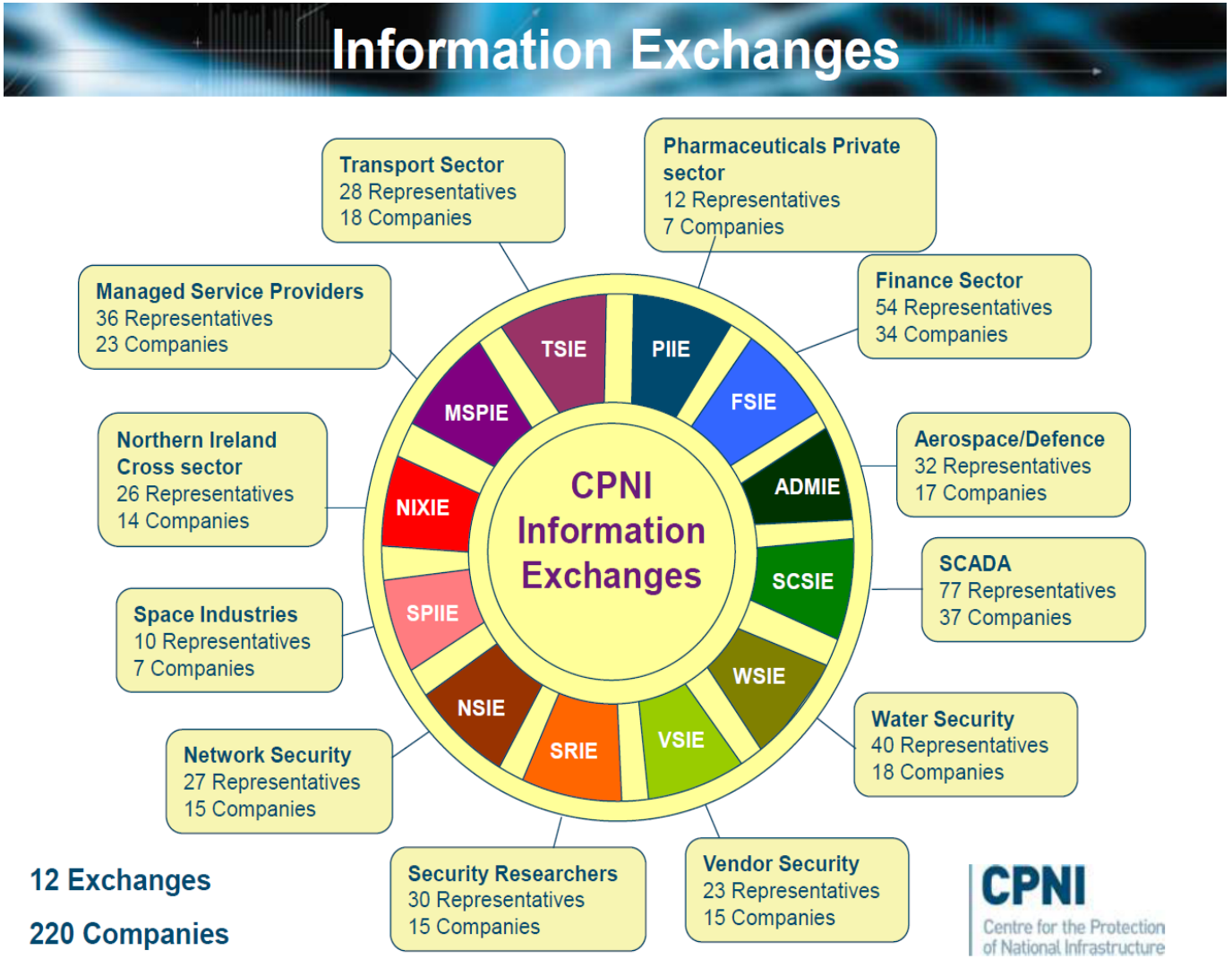
- Industry:
  - Fixed-line telecommunications CSPs
  - Mobile telecommunications CSPs
  - The Internet peering community
  - Major Data Centres
- Government:
  - Cabinet Office
  - BIS
  - CPNI
  - Home Office
  - MoD
  - Regional Government Offices
- Ofcom - National Sector Regulator

- National Emergency Alert for Telecoms (NEAT)

Examples of Information Exchanges

- CPNI UK
  - Network Security Information Exchange (NSIE)
- CPNI Netherlands
  - Telecom-ISAC
- EU-wide
  - EuroSCSIE (SCADA)
- USA
  - IT-ISAC

Information Exchanges in the UK



What is trust?

- The belief that someone or something is reliable, good, honest, effective, etc. (Merriam-Webster)
- A powerful enabler
- Allows an organisation to carry out specific tasks whilst another organisation carries out complementary tasks
- It saves time finding out or checking
- Teams, partners and organisations learn to trust each other
- Can achieve more with less resources

but . . .

- Trust has its limits, so needs careful scoping
- Trust can be very strong, but is fragile – easily broken and very difficult to repair

Whom should we trust?

- The Government
- The Sector Regulator
- Our business partners
- Our competitors

What should we trust them with?

- Commercially-sensitive information
- Technical information
- Security information

How should we share this information?

- Openly or anonymously
- Freely, or with certain restrictions
- One-to-one or multi-party
- One-way or both-way
- Cross-sector
- Cross-border

Traffic Light Protocol (TLP)

- **WHITE** - Unlimited - Subject to standard copyright rules, WHITE information may be distributed freely and without restriction.
- **GREEN** – Community-Wide - Information in this category can be circulated widely within a particular community or organisation. However, the information may not be published or posted on the Internet, nor released outside of the community.
- **AMBER** - Limited Distribution - Recipients may share AMBER information with others within their organisation, but only on a 'need-to-know' basis. The originator may be expected to specify the intended limits of that sharing.
- **RED** - Personal for Named Recipients Only - In the context of a meeting for example, distribution of RED information is limited to those present at the meeting, and in most circumstances will be passed verbally or in person.

The European perspective

- COM(2004) 702 – recognised the vulnerabilities of critical infrastructures
- Regulation 460/2004 set up the European Network and Information Security Agency (ENISA)
- Green Paper COM(2005) 576 – set out the requirements for a European Programme for Critical Infrastructure Protection
- COM(2006) 251 – recommended 'European multilingual information sharing and alert system'
- The Availability and Robustness of Electronic Communications Infrastructures (ARECI) Report (2007)

ARECI recommendations

1 Emergency preparedness

2 Priority communications on public networks

3 Formal mutual aid agreements

4 Critical infrastructure information sharing

5 Inter-infrastructure dependencies

6 Supply chain integrity and trusted operation

7 Unified European voice in standards

8 Interoperability testing

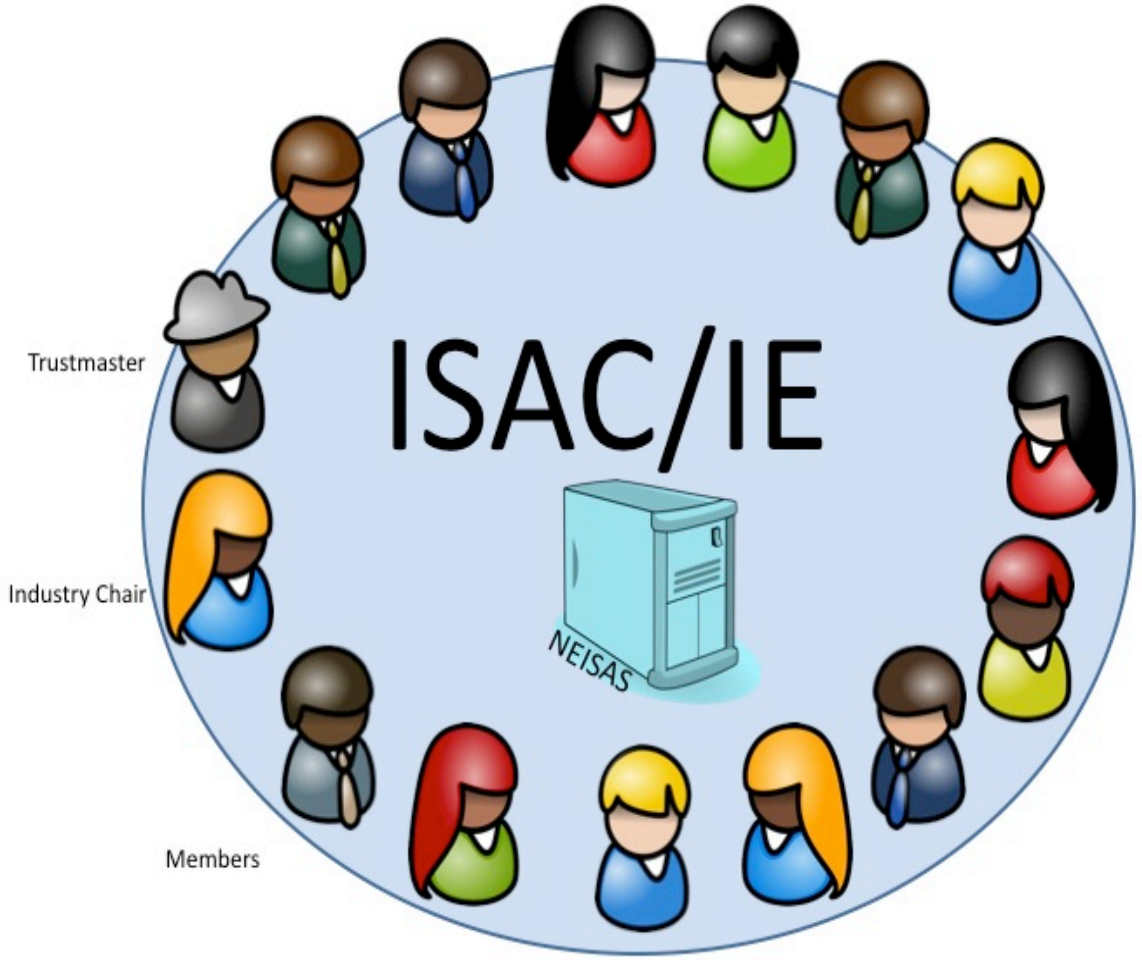
9 Vigorous ownership of partnering health

10 Discretionary European best practices

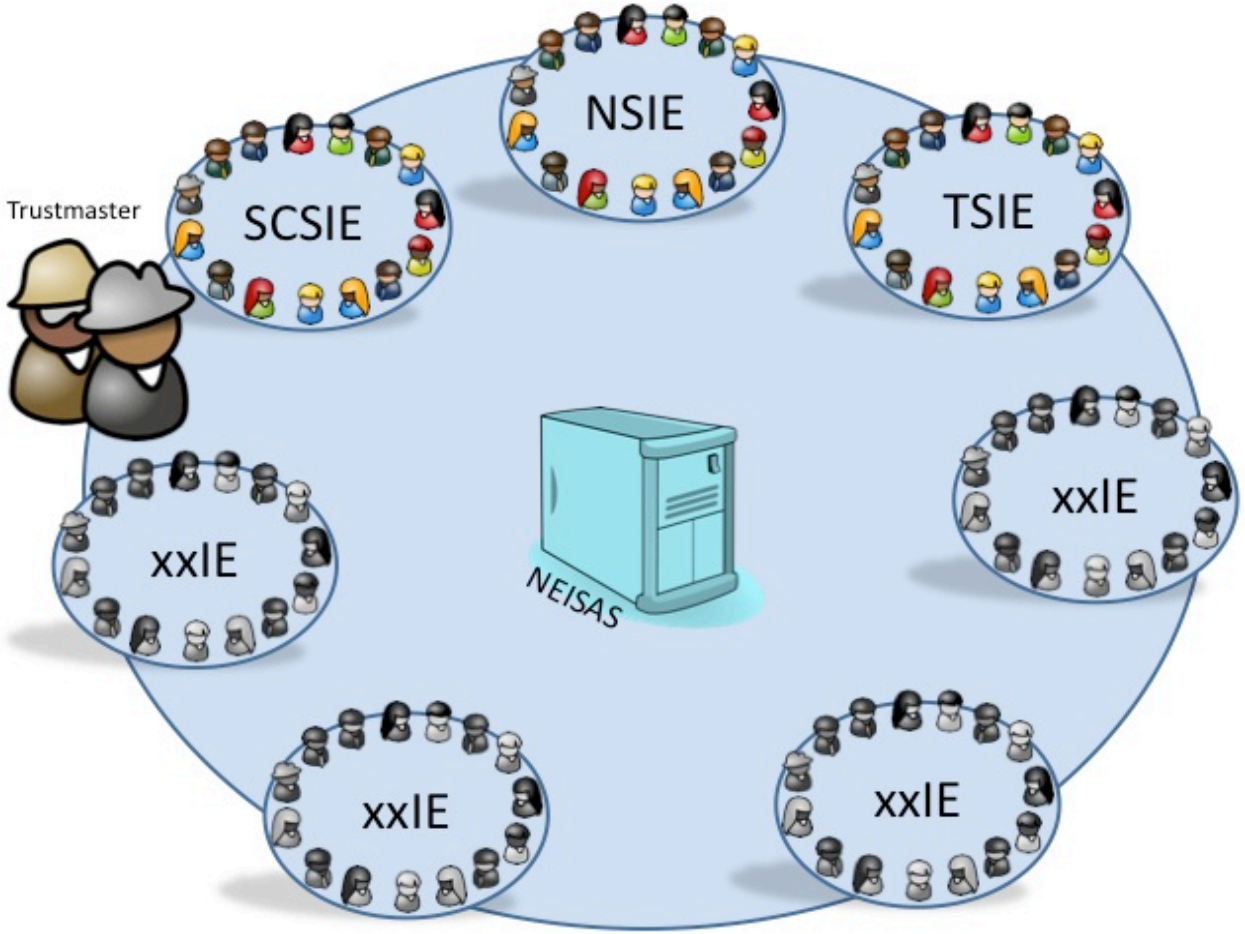
NEISAS (2009 – 2011)

- The development of a model and a pilot platform for a National and European Information Sharing and Alerting System
- Co-funded by The European Commission, Directorate General for Justice, Freedom and Security (DG JLS) as part of EPCIP
- Consortium of Italian National Agency for new technologies (ENEA), Booz & Co., LanditD
- Secure, nationally-based platforms in Italy, the UK & the Netherlands
- Uses a common approach to Secure Information Sharing (ISO/ IEC 27010:2012)

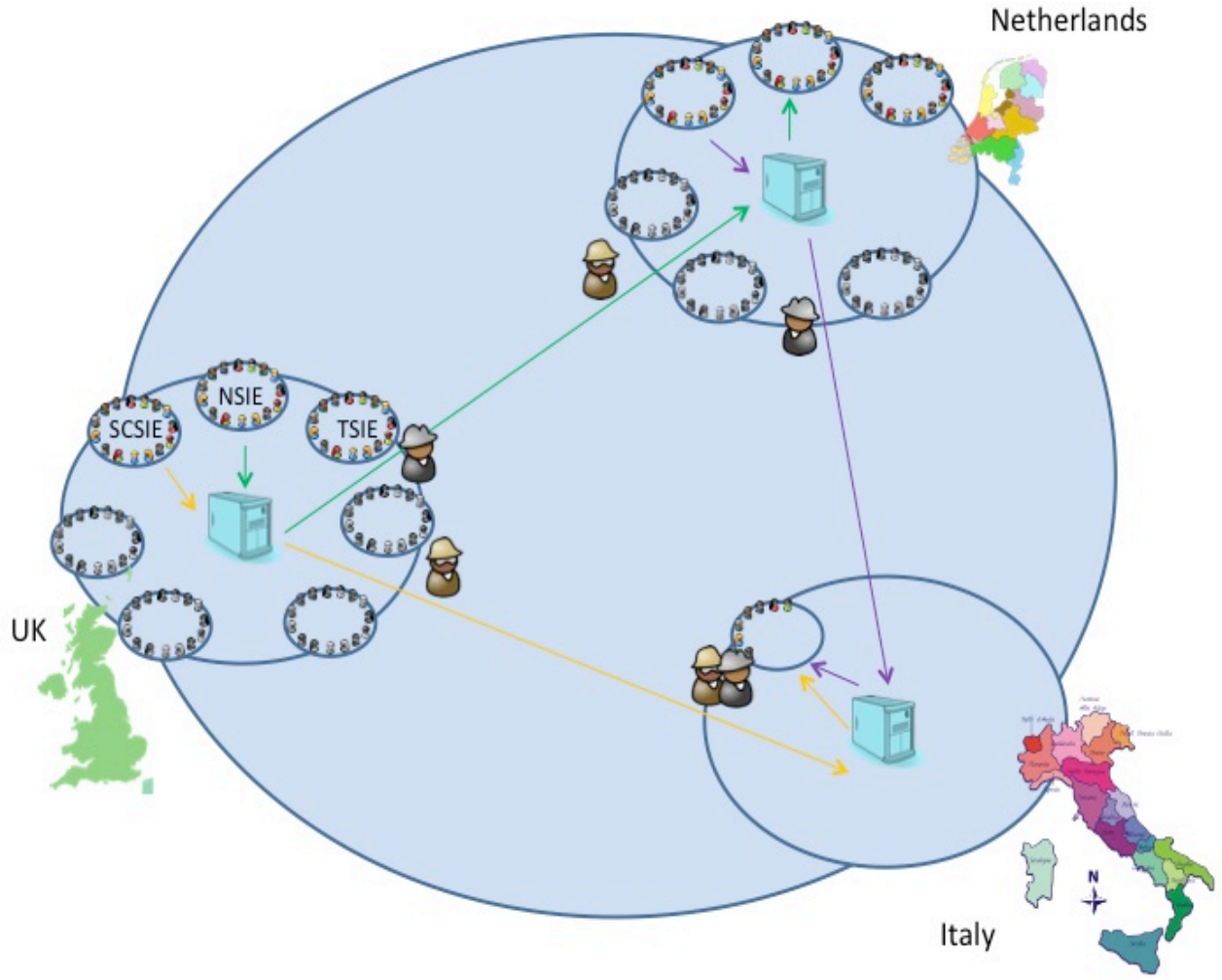
Single circle of trust



Multiple circles of trust



Cross-border sharing



Benefits of an information sharing mechanism

- Supports the Traffic Light Protocol (TLP)
- Provides anonymity
- Supports Information Rights Management
- Permits cross-border sharing
- Watch the movie at www.neisas.eu/

Questions ?

David Sutton FBCS SBCI M. Inst. ISP CISSP

tacit.tel
consulting