Industry and the SCSIE

Tony Phipps EDF Energy – Past Chair

Bill Fulton SP EnergyNetworks – Current Chair

Sandra C – CPNI coordinator

12th Oct 2010

SCSIE

- **S**CADA and
- **C**ontrol
- **S**ystem
- **I**nformation
- **E**xchange

SCSIE

"A confidential industry forum that meets regularly to exchange information on SCADA threats, incidents and mitigation"

UK Government

- NISCC
  - NATIONAL Infrastructure Security Coordination Centre
  - Electronic
- CPNI
  - Centre for the Protection of the National Infrastructure
  - Electronic, Physical and Personnel

Development of the UK SCSIE

- Past
- Current
- Future

SCSIE – The Past

Establishing the SCSIE

- Officially founded under NISCC on 17th Oct 2003
- Articles of Association “SCSIE-UK”
- Allowed 2 or 3 attendees per company
- Meetings held bi-monthly hosted by NISCC

SCSIE Membership

- Industry
  - Control Systems engineers
  - Control Systems security staff
  - Corporate IT security personnel
  - Corporate Security (non IT)
  - No contractors
- NISCC/CPNI
  - Security advisors – energy, water, transport

What NISCC brought

- New members pre-check
  - carried out by NISCC
- Honest broker
- Stable executive for group
- Traffic Light Protocol
- Central Point of Contact

What SCSIE members brought

- Chalk and talk presentations
- Pro-active round table discussions
- Knowledgebase
- Deeper understanding of impact of security issues in SCADA and PLC environments
- Understanding of problems resulting from application of security in SCADA & PLC environments

How the SCSIE evolved

- Established
  - Working Groups
  - Vendor Survey
  - Assurance Matrix
- Used Members willingness to contribute
  - *Members had more time to devote to the SCSIE*

What NISCC gained

- First time UK Govt had actual in depth knowledge of SCADA & PLC industry (without employing consultants)
- NISCC/CPNI gained valuable direct contacts direct in CNI operators
- A trusted and important two-way relationship

SCSIE Values

- Need to add value to Industry and Government
- Everyone needs to get something from the relationship
- Honest relationships - no hidden agendas

SCSIE Early Milestones

- NISCC SCADA Threat Assessments 2003 onwards
- SCADA Security Conferences 2003, 2004 & 2005
- “CEO” Conferences 2006 & 2007
- Firewall Deployment Guide 2004
- Good Practice Guides 2005

SCSIE benefits

- Working Groups
  - Benchmarking
  - Secure Remote Access
  - SCADA/PLC and move to IP
  - Security over IP
- Policy Review
- Joint & Inter-IE Activity
- Business Case Support
- New Architecture Standard

SCSIE benefits

- New Architecture Standard
- SSAT / Internal Audit
- Personnel, Travel & Protective Security
- Proposed CEO Briefing session

Launch of CPNI

- Formed in 2007
- Merging of NISCC and NSAC (physical and personnel security) into CPNI
- Provides Holistic approach to security

SCSIE – The Present

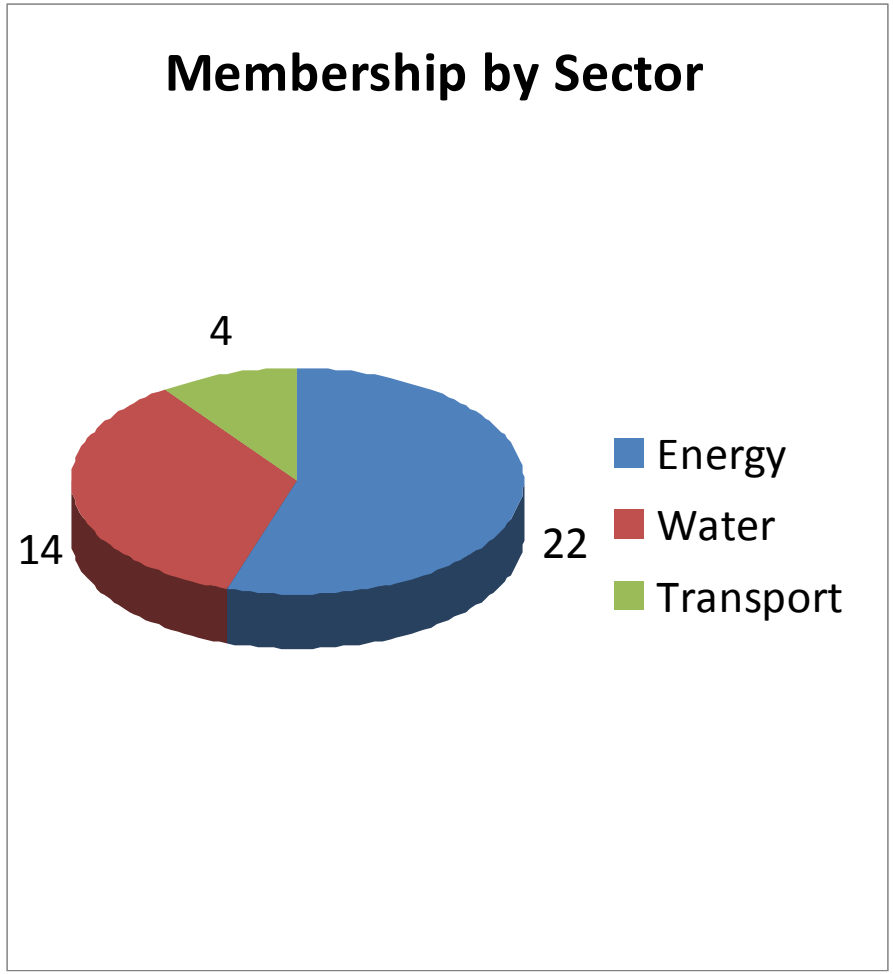
SCSIE today

- Has a full time CPNI SCSIE co-ordinator
- Rotating annual Industry Chair / Vice Chair
- Current Membership 40+ Companies
- Meetings held quarterly
- Had to restrict attendance per company
- Working Groups being supplemented by external parties.

SCSIE today

- Current Membership (2010)

  40 companies
  - Energy
    - Electricity
    - Gas
    - Petroleum
  - Water
  - Transport



SCSIE today

- Range of size of members
  - Small Water company
  - International Petrochemical company
- Spread of Different industries
  - Energy & Water
  - Petrochemical
  - Transport
- Common areas of concern

What Industry brings to the SCSIE

- Depth of experience in operation of SCADA & PLC systems
  - Broad spectrum of UK CNI represented
- Business threat Intelligence
- Actual Incidents
- Near Misses
- Understanding of “real world”

What Industry receives from the SCSIE

- CPNI guidance on Best Practice
- Actual best practice presentations by other members
- Threat visibility across a broad spectrum
  - Informed by access to intelligence
- Actual incidents and opportunity to use knowledge to improve own position
- Networking across industries

What Industry receives from the SCSIE

- Sensitive information from CPNI
  - Known and trusted community
- Information from other members
- Information from vendors
- NETWORKING

Drawing up a SCSIE agenda

- **Jointly** in face to face pre-meeting
  - SCSIE Industry Chair
  - SCSIE Industry Deputy Chair
  - CPNI Chair
  - CPNI Co-ordinator

A typical SCSIE Agenda

- Introductions, Minutes & Actions
- Round Table
- Presentations by Members
- Presentations by CPNI
- Presentations by 3rd Party

SCSIE Current Milestones

- SSAT questionnaire
- CPNI Good Practice Guides
- CPNI Technical Papers
- Other material for SCSIE members only

SCSIE – The Future

What could industry improve ?

- Get the most appropriate SCADA/PLC security member of staff at the SCSIE
- Collect more information from colleagues to bring to SCSIE
- Share more from the SCSIE with colleagues
- Greater Euro-SCSIE and MPCSIE involvement

What could CPNI improve ?

- Provide more detailed information on actual incidents from around the world
  - Industry would like more information!
  - Relate to business issues
  - Composed into business speak
- Share more information from partners

Challenges

- Achieving greater input from Industry
- Industry is more demanding for information
- Impact of Regulation

Pros & Cons

- Partnership v policing
- Sharing v hiding
- Ownership v tick sheet
- Compliance v best practice
- Stable v dynamic

Key Risks

- Risk – outsourcing personnel
- Risk – outsourcing services
- Risk – global ownership of companies

- All risks can be managed

Member Company changes

- More UK CNI companies are not now UK owned
- Issues are becoming more global
- Attackers can be from anywhere in the world
- Attacks may impact but not be directed at UK CNI

Threat – the changes

- More knowledge publically available
  - Incidents featuring in mainstream press
  - Hollywood film exposure
- SCADA security now has it’s own industry
  - Good guys and bad guys
  - Hackers (Black hat) are interested
- Environmentalists focusing on electronic attacks

Development of CPNI Extranet

- Original version was one way
- New version will have new information sharing tools
  - CPNI to Industry
  - Industry to CPNI

SCSIE – new developments

- Working with ICS vendors
- Smart meters and smart grids
- Further research
- More GPG
- Increase memberships – wind farms, building management systems, alarms systems.
- SCSIE spinning of new IEs focussing on related areas ?
- Fast track an new IE to maturity, is it possible ?

SCSIE – new developments

- SCADA signatures
- SCADA IPS
- Bite size affordable SCADA security training
- Emulation of default vendor password and account
- More SCADA security testing

SCSIE – new developments

- Should SCSIE or CPNI develop
  - Templates for SCADA Risk Assessment
  - Templates for SCADA BCP and Disaster Recovery
  - High level procurement advice
  - More publically available GPG

SCSIE – new developments

- New technologies potentially impacting on SCADA & PLCs
  - Cloud computing
  - VoIP
  - IPv6
  - Encryption v latency

SCSIE Future Milestones

- SCADA Firewall Good Practice Guide – 2011
- CPNI GPG, Security Assessments, Remote Access and move to IP networks.
- CPNI producing supporting materials (non technical)
  - Easier to transfer to corporate world

SCSIE Future Milestones

- Security assessments carried out in UK
- Common areas of vulnerabilities
  - Increased knowledge
  - Solutions

SCSIE
Why will it continue to work ?

- Trust built slowly
- Share and assist (engineering sharing culture)
- Equal relationship between Industry and Government Authorities/Advisers
- Everyone has to contribute

SCSIE
Why will it continue to work ?

- CPNI is independent and not a regulator/policy-setter
- But CPNI is a Government Authority with direct link into Government Departments when required

SCSIE
Why will it continue to work ?

- Membership – no consultants
- A forum for industry, that is facilitated by CPNI (no cost to members)
- A forum for industry that is invitation only

SCSIE
Why will it continue to work ?

- Industry and CPNI jointly decided on scope required for research/good practice
  - Documents reviewed by both parties
  - Industry leads on working groups
- Careful managing by CPNI of 3rd parties invited into meetings
- And finally....

Common desire for success

QUESTIONS

Tony Phipps EDF Energy – Past Industry Chair
Tony.Phipps@edfenergy.com

Bill Fulton SP – Current Industry Chair
Bill.Fulton@sppowersystems.com

Sandra C - CPNI coordinator
sandrac@cpni.gsi.gov.uk