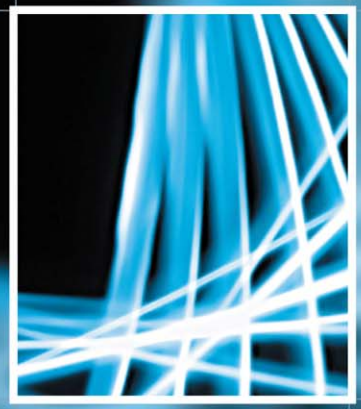


SCADA SAT (SSAT) - UK

Sandra C Security Adviser Energy
Dan B Security Adviser Water

CPNI
Centre for the Protection of National Infrastructure

Who we are?

What is the SSAT?

Personnel experience of deploying the SSAT

CPNI
Centre for the Protection of National Infrastructure

Centre for the Protection of National Infrastructure

CPNI provides integrated (electronic, personnel and physical) security advice to the businesses and organisations which make up the national infrastructure.

CPNI
Centre for the Protection of National Infrastructure

CPNI SCADA team

Security Advisors – not auditors.

Energy (Electricity, Oil & Gas), Water, Transport, (Food & Health)

CPNI
Centre for the Protection of National Infrastructure

No NERC CIP in UK

UK has SCADA Good Practice Guides

Pros and Cons – can be discussed for ever

CPNI
Centre for the Protection of National Infrastructure

Why do we need a SSAT

Good Practice published - 2005

Are UK utilities using it?

Can we measure the % of Good Practice in the UK?

SSAT first sent out 2008

CPNI
Centre for the Protection of National Infrastructure

Questions are based the CPNI Good Practice Guidance and Cyber Security Procurement Language for Control Systems

Question set have been reviewed by UK Industry

CPNI
Centre for the Protection of National Infrastructure

Good Practice Guide: Process Control and SCADA Security

Available on CPNI public website www.cpni.gov.uk search SCADA

Guide 1. Understand the business risk
Guide 2. Implement secure architecture
Guide 3. Establish response capabilities
Guide 4. Improve awareness and skills
Guide 5. Manage third party risk
Guide 6. Engage projects
Guide 7. Establish ongoing governance
Firewall Deployment for SCADA and Process Control Networks

Plus
Cyber Security Procurement Language for Control Systems
CPNI Personnel Security Measures

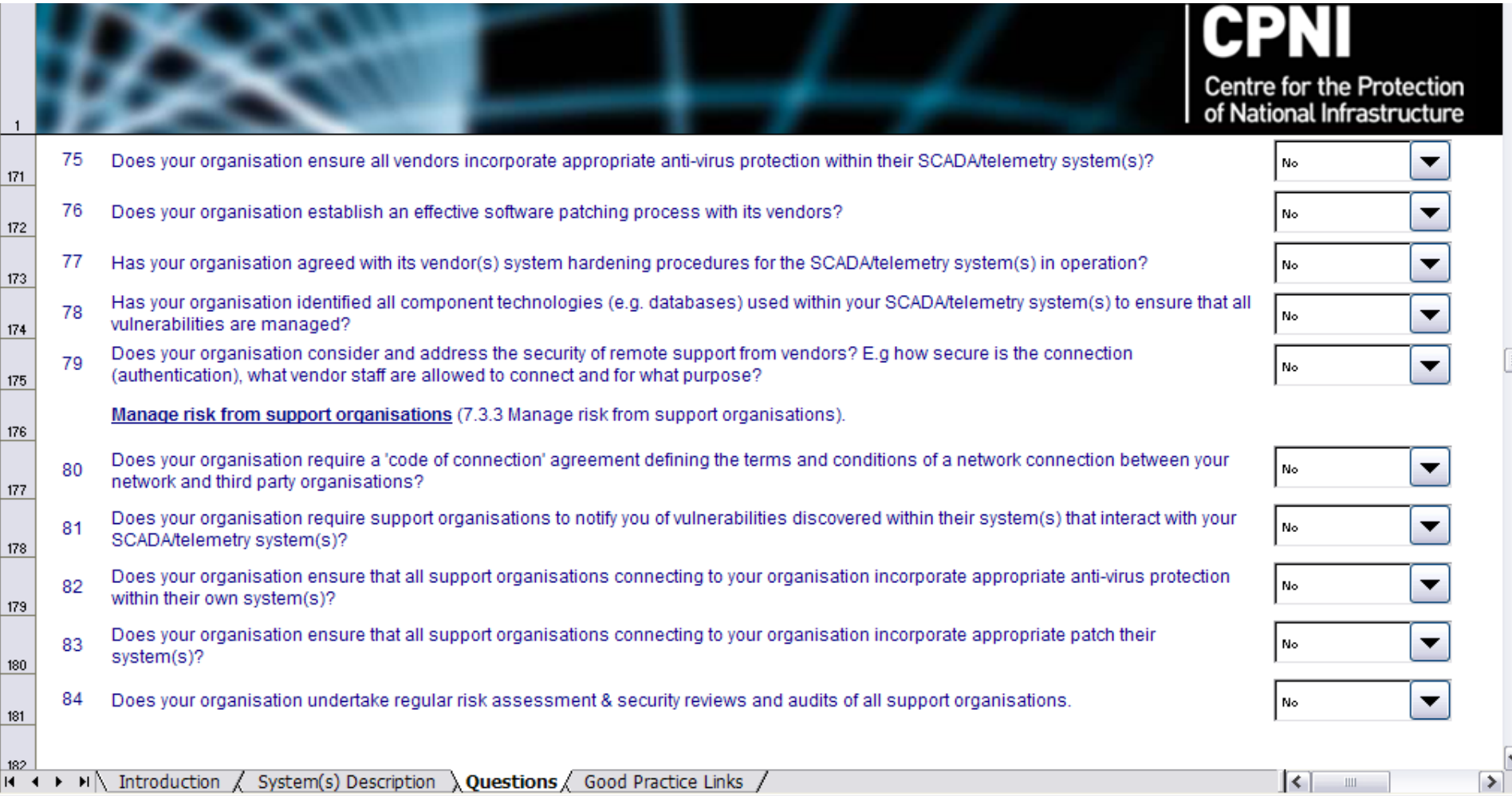
CPNI
Centre for the Protection of National Infrastructure

SSAT Overview

- 99 questions
- Physical, Personnel and Electronic
- Based upon CPNI, Industry and International good practice
- “The SSAT seeks to provide a high level snap-shot of the information assurance of an organisation’s industrial control system(s) that are deemed to constitute (directly or indirectly) the UK critical national infrastructure. It is intended that the SSAT be completed on an annual basis by UK CNI companies across the relevant sectors to enable comparisons overtime and across industries. The SSAT links directly to the CPNI SCADA security good practice. “

CPNI
Centre for the Protection of National Infrastructure

SCADA Self Assessment Tool



Why do we use it?

High level understanding of level of protective for SCADA/ICS assets in the UK

‘Door opener’ for further discussion, and joint working to improve protective security

CPNI
Centre for the Protection of National Infrastructure

What it does not do

Answers/scoring is not weighted.

Yes/No/Sometimes answers plus text boxes

Not a standalone assessment tool

CPNI
Centre for the Protection of National Infrastructure

Scoring – Tfc light - % of good practice

Green – 85% or more	
Amber – 60 to 84%	
Red – 59% or less	

CPNI
Centre for the Protection of National Infrastructure

- Companies report will contain their own scoring
- Scoring from the previous year

- Plus a average score from their sector

- A list of recommendations

CPNI
Centre for the Protection of National Infrastructure

Common findings

- Companies need to conduct a threat assessment
- Should understand impacts if threats realised
- Should identify a senior manager responsible for SCADA/Telemetry networks
- Should have a managerial member with defined responsibility for SCADA/Telemetry networks

CPNI
Centre for the Protection of National Infrastructure

- Should ensure all connections to SCADA/Telemetry networks have a business case
- Should have a change control process
- Should have a documented password policy
- Should have a starters and leavers policy
- Verify devices are free from malware before connecting
- Should have a SCADA/Telemetry staff awareness programme
- Develop a forum between SCADA/Telemetry and corporate IT teams can share knowledge

- Verify devices are free from malware before connecting
- Should have a SCADA/Telemetry staff awareness programme
- Develop a forum between SCADA/Telemetry and corporate IT teams can share knowledge
- Should review CPNI guidance on managing third party risk
- Should engage with projects to identify implications for SCADA/Telemetry networks are identified

CPNI
Centre for the Protection of National Infrastructure

Outcomes

Process – Now moving into 3rd year

SSAT question set – v3.1

(input and review by Industry)

Improvement - average increase of performance –

40% (electricity sector)

Well received by all companies and UK Government

CPNI

Centre for the Protection of National Infrastructure

What are the results used for

- Sector aggregated results reported to UK Government
- Benchmarking
- Shows areas of weakness/vulnerabilities
  - Who should solve these?
    - Industry
    - Government
    - CPNI
    - Or all three

CPNI
Centre for the Protection of National Infrastructure

Future

- Use internally by UK Utilities

- Not for public release
  - Never design for this
  - Scoring not weighted
  - Not robust enough
  - Never the aim

.

CPNI
Centre for the Protection of National Infrastructure

BUT

If anyone would like to design a publically available Scada Self Assessment Tool, that links direct to SCADA Good Practice,

Please do

CPNI
Centre for the Protection of National Infrastructure

SSAT - Benefits

- Electronic Security Background

- Corporate / Government Systems
  - Heavily regulated
  - Accreditation
  - Incidents to ‘focus the mind’

- Minimal experience of Control Systems

CPNI
Centre for the Protection of National Infrastructure

One year of working with SSAT

- Initial impressions of ICS Security were poor
  - Existing guidance (passwords, group accounts)
  - Impressions from research (Wikipedia)
    - the lack of concern about security and authentication in the design, deployment and operation of existing SCADA networks
    - SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces
    - SCADA networks are secure because they are physically secured
    - SCADA networks are secure because they are disconnected from the Internet
  - 10 years behind the curve
- Initial returns from SSAT worrying
  - Patching policy (What?)
  - Legacy kit
  - Network design

CPNI
Centre for the Protection of National Infrastructure

But with experience and Time..

- Meetings with Companies
  - Availability rather than confidentiality
  - Cost constraints
  - Equipment lifecycle – 20 years +
  - Threat Awareness
  - Use of corporate technology but none of the security methods (AV, Intrusion Detection)
- Better understand Companies
  - Mechanism for closer involvement

CPNI
Centre for the Protection of National Infrastructure

In average terms, an improvement in every area:

	SECTOR 2009
1) Understand the Business Risk (max=10)*	Up 9%
1a) Understand the Vulnerabilities (max=10)*	Up 27%
2) Establish Ongoing Governance (max = 5)	Up 21%
3) Implementing Secure Architecture	
Perimeter Defence (max =26)	Up 16%
Malware Protection (max=16)	Up 8%
Insider Threat (max=9)	Up 22%
Security Management (max=3)	Up 10%
Backups and recovery (max=3)	Up 7%
Physical Security (max=6)	Up 12%
4) Improve Awareness and Skills (max=5)	Up 17%
5) Establish Response Capabilities (max=5)	Up 2%
6) Manage Third Party Risk (max=16)	Up 4%
7) Engage Projects (max=4)	Up 20%
8) Procurement (max=5)	N/A

CPNI
Centre for the Protection of National Infrastructure

In average terms, an improvement in every area:

	SECTOR 2009
1) Understand the Business Risk (max=10)*	**Up 9%**
1a) Understand the Vulnerabilities (max=10)*	**Up 27%**
2) Establish Ongoing Governance (max = 5)	**Up 21%**
3) Implementing Secure Architecture	
Perimeter Defence (max =26)	Up 16%
Malware Protection (max=16)	Up 8%
Insider Threat (max=9)	Up 22%
Security Management (max=3)	Up 10%
Backups and recovery (max=3)	Up 7%
Physical Security (max=6)	Up 12%
4) Improve Awareness and Skills (max=5)	Up 17%
5) Establish Response Capabilities (max=5)	Up 2%
6) Manage Third Party Risk (max=16)	Up 4%
7) Engage Projects (max=4)	Up 20%
8) Procurement (max=5)	N/A

CPNI
Centre for the Protection of National Infrastructure

In average terms, an improvement in every area:

	SECTOR 2009
1) Understand the Business Risk (max=10)*	Up 9%
1a) Understand the Vulnerabilities (max=10)*	Up 27%
2) Establish Ongoing Governance (max = 5)	Up 21%
3) Implementing Secure Architecture	
Perimeter Defence (max =26)	Up 16%
Malware Protection (max=16)	Up 8%
Insider Threat (max=9)	**Up 22%**
Security Management (max=3)	Up 10%
Backups and recovery (max=3)	Up 7%
Physical Security (max=6)	Up 12%
4) Improve Awareness and Skills (max=5)	**Up 17%**
5) Establish Response Capabilities (max=5)	Up 2%
6) Manage Third Party Risk (max=16)	Up 4%
7) Engage Projects (max=4)	Up 20%
8) Procurement (max=5)	N/A

Personnel security work

CPNI
Centre for the Protection of National Infrastructure

Highlighted work to do

- SSAT will adapt/improve year by year
  - Threats and technology change
- Improvements still to be made
  - Change control
  - Working with vendors
  - Threat awareness
  - Remote Access solutions

CPNI
Centre for the Protection of National Infrastructure

Questions?

CPNI
Centre for the Protection of National Infrastructure

Thank you

sandrac@cpni.gsi.gov.uk
danba@cpni.gsi.gov.uk

www.cpni.gov.uk

CPNI
Centre for the Protection of National Infrastructure