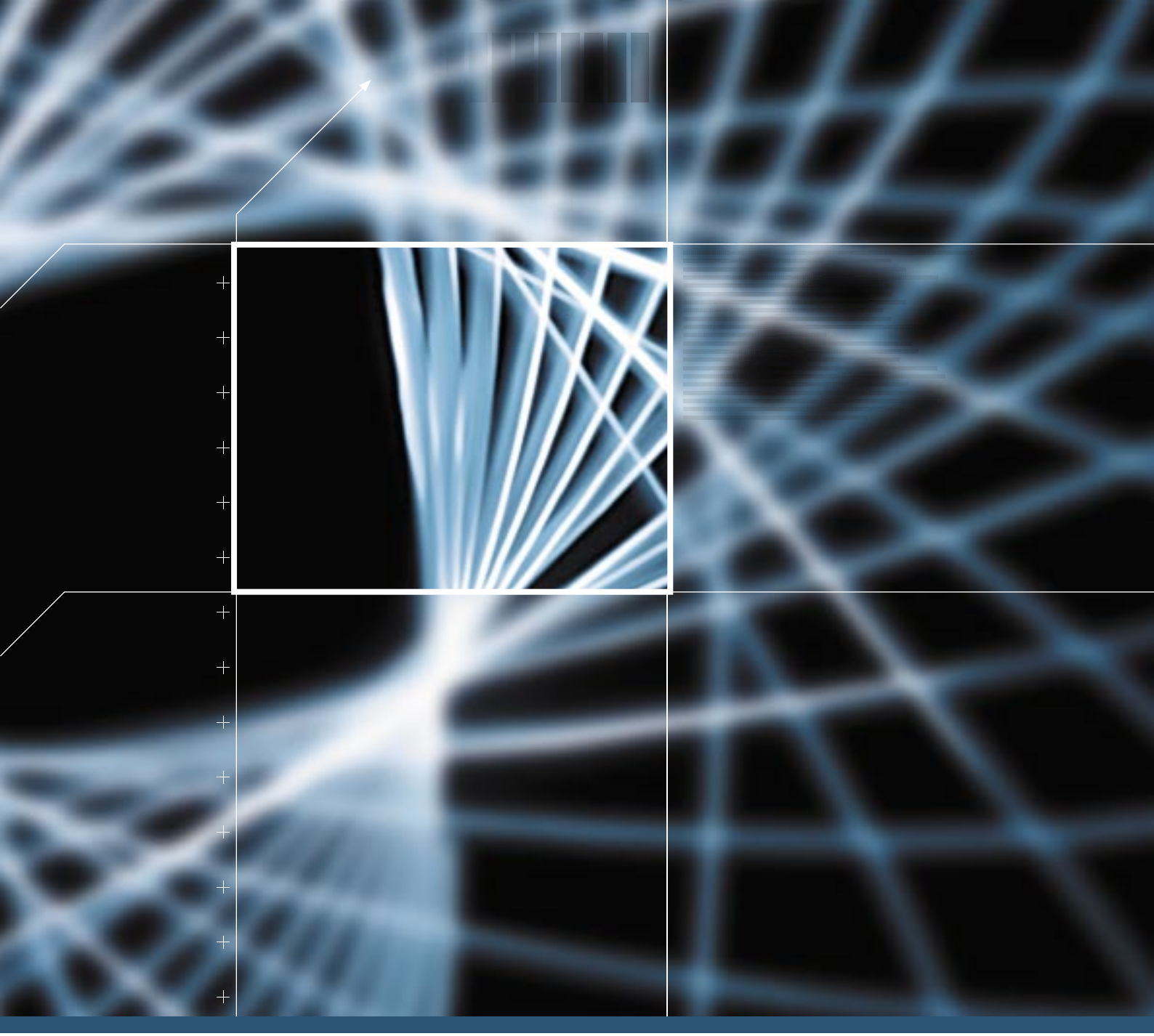

GOOD PRACTICE GUIDE

PROCESS CONTROL AND SCADA SECURITY

GUIDE 3. ESTABLISH RESPONSE CAPABILITIES

CPNI
Centre for the Protection of National Infrastructure

This guide is designed to impart good practice for securing industrial control systems such as: process control, industrial automation, distributed control systems (DCS) and supervisory control and data acquisition (SCADA) systems. Such systems are used extensively across the nation's critical national infrastructure. The paper provides valuable advice on protecting these systems from electronic attack and has been produced by PA Consulting Group for CPNI.

TABLE OF CONTENTS

1. Introduction 2

1.1 Terminology 2

1.2 Background 2

1.3 Process control security framework 2

1.4 Purpose of this guide 3

1.5 Target audience 3

2. Establish response capabilities summary 4

3. Establish Response Capabilities 5

3.1 Context of this section within the overall framework 5

3.2 Rationale 6

3.3 Good practice principles 6

3.4 Good practice guidance 6

3.4.1 Create a Process Control Security Response Team (PCSRT) 6

3.4.2 Establish security response and continuity plans 8

3.4.3 Key contents of a incident response plan 9

3.4.4 Ensure plans are regularly maintained, rehearsed and tested 9

3.4.5 Establish an early warning system 9

3.4.6 Establish processes and procedures 14

3.4.7 Establish incident reporting 16

3.4.8 Ensure lessons are learned from incidents 16

Appendix A: Document and website references 17

General SCADA references 18

Acknowledgements 21

1. INTRODUCTION

1.1 Terminology

Throughout this framework the terms process control system and process control and SCADA system are used as generic terms to cover all industrial control, process control, distributed control system (DCS), supervisory control and data acquisition (SCADA), industrial automation and related safety systems.

1.2 Background

Process control and SCADA systems are making use of, and becoming progressively more reliant on standard IT technologies. These technologies, such as Microsoft Windows, TCP/IP, web browsers and increasingly, wireless technologies, are replacing conventional proprietary technologies and further enabling bespoke process control systems to be replaced with off the shelf software.

Although there are positive business benefits to be gained from this development, such a transformation brings with it two main concerns:

Firstly process control systems were traditionally only designed for the purpose of control and safety. Due to the need for connectivity for example for the extraction of raw plant information or for the ability to perform direct production downloads, the once isolated systems are being connected to larger open networks. This exposes them to threats that these systems where never expected to encounter such as worms[1], viruses and hackers. Security through obscurity is no longer a suitable kind of defence.

Secondly, commercial off the shelf software and general-purpose hardware is being used to replace proprietary process control systems. Many of the standard IT security protection measures normally used with these technologies have not been adopted into the process control environment. Consequently, there may be insufficient security measures available to protect control systems and keep the environment secure.

There are potentially serious consequences should these vulnerabilities be exploited. The impacts of an electronic attack on process control systems can include, for example: denial of service, unauthorised control of the process, loss of integrity, loss of confidentiality, loss of reputation and health, safety and environmental impacts.

1.3 Process control security framework

Although process control systems are now frequently based on standard IT technologies, their operational environments differ significantly from the corporate IT environment. There are a great number of lessons that can be learned from the experiences gained by the IT security experts and after tailoring some standard security tools and techniques can be used to protect process control systems. Other standard security measures may be completely inappropriate or not available for use in a control environment.

[1] The Wikipedia reference for a worm – A computer worm is a self replicating computer program. It uses a network to send copies of itself to other systems and it may do so without user intervention. Unlike a virus, it does not attach itself to an existing program. Worms always harms the network (if only consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.

This process control security framework is based on industry good practice from the fields of process control and IT security. It focuses on seven key themes to address the increased use of standard IT technologies in the process control and SCADA environment. The framework is intended to be a point of reference for an organisation to begin to develop and tailor process control security that is appropriate to its needs. The seven elements of the framework are shown below in Figure 1.

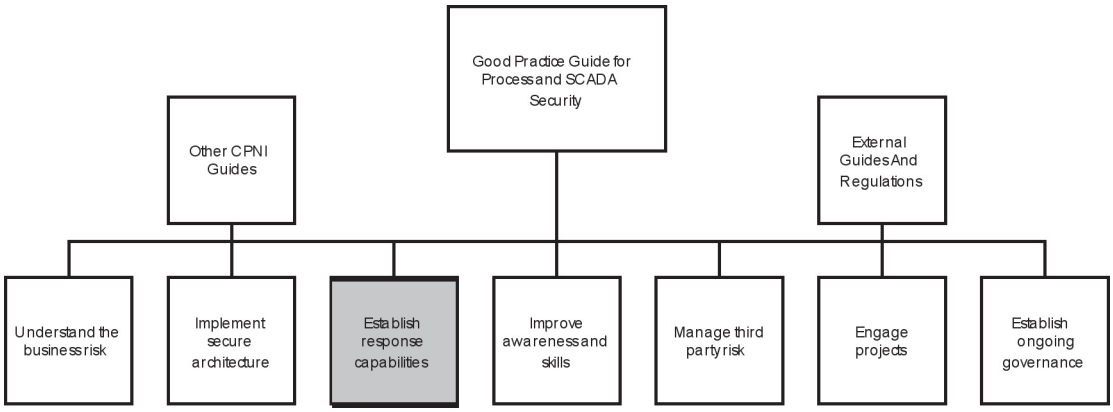

Figure 1 – Where this guide fits in the Good Practice Guide framework

Each of these elements is described in more detail in their separate documents, this document provides good practice guidance on understanding the business risk. All the documents in the framework can be found at the following link http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx .

1.4 Purpose of this guide

The CPNI **'Good Practice Guide - Process Control and SCADA Security'**, proposes a framework consisting of seven elements for addressing process control security. This **'Establish response capabilities'** guide builds on the foundation provided in the high level framework guide and provides guidance on establishing response capabilities relating to digital security threats in process control and SCADA systems.

This guide does not provide detailed response plans or procedures as these will vary from organisation to organisation and system to system.

1.5 Target audience

This guide is aimed at anyone involved in the security of process control, SCADA and industrial automation systems including:

- Process control and automation, SCADA telemetry engineers
- Information security specialists
- Physical security specialists
- Business leaders
- Risk managers
- Health and safety officers
- Operations engineers
- Security response teams.

2. ESTABLISH RESPONSE CAPABILITIES SUMMARY

Organisations in the process control environment will already have disaster recovery (DR) and business continuity plans (BCP) in place. However, due to changes in the process control operational environment as already discussed, these plans are often inadequate to cater for electronic attack threats.

Security protection measures cannot provide 100 per cent protection to systems because both technical and non-technical vulnerabilities will continue to exist regardless of the protective security regime. An essential part of any security strategy is therefore to recognise that residual risks to systems will continue to exist and have to be managed along with the ability to identify and respond to any other changes in the threat.

Analysis indicates that process control security incidents from an electronic attack perspective were a rare occurrence and caused minimal disruption. Such incidents are now becoming more frequent[2] and organisations have to plan for them, both by revising their protective security regime and by developing or reviewing incident response policies and procedures.

One of the issues that has to be considered is that normal information assurance approaches as applied to the office environment may not be suitable for process control systems. Such systems often face different challenges and constraints. Although the differences may be subtle, it is important to consider them when developing the information security requirement and preparing incident response plans in particular.

An example is the application of security patches or software updates where process control system vendors often need to test and accredit patches prior to their deployment on live systems. During this time, the systems may be vulnerable to attack – hence the need to consider the potential threat from not patching and the need for suitable countermeasures.

Another example is that these systems often directly control safety critical equipment and if an intruder is detected then the usual response is to isolate the compromised system so that the equipment may continue its role without interference. With traditional IT systems, the response may be to allow the attacker to remain in the system but monitor their activities to gather intelligence for a possible prosecution or gain an understanding of the vulnerability or exploit that was used to gain access to the system.

Throughout this good practice framework, three guiding principles have been used. These principles are protect, detect and respond. The majority of the guides within the framework are concerned with protecting process control systems by deploying a variety of security measures. This guide focuses on detecting potential incidents and deploying appropriate responses to minimise the extent and impact of any incident or avoid them completely.

[2] 70 per cent of security incidents in the period 2001-2003 were external generated compared with 31 per cent between 1982 and 2000. 41 per cent of incidents resulted in the loss of production, a further 29 per cent reported a loss of viewing of the process – The Myths and Facts behind Cyber Security Risks for Industrial Control Systems – Eric Byres & Justin Lowe

3. ESTABLISH RESPONSE CAPABILITIES

3.1 Context of this section within the overall framework

Establishing effective incident response capabilities is tightly linked with all other elements of this good practice guidance framework. The ability to respond effectively to security events will depend on the ability to monitor and detect security related events and the quality of the response plans in place. This in turn is dependent upon well secured and monitored systems, effective and clear governance and the skills and awareness of personnel.

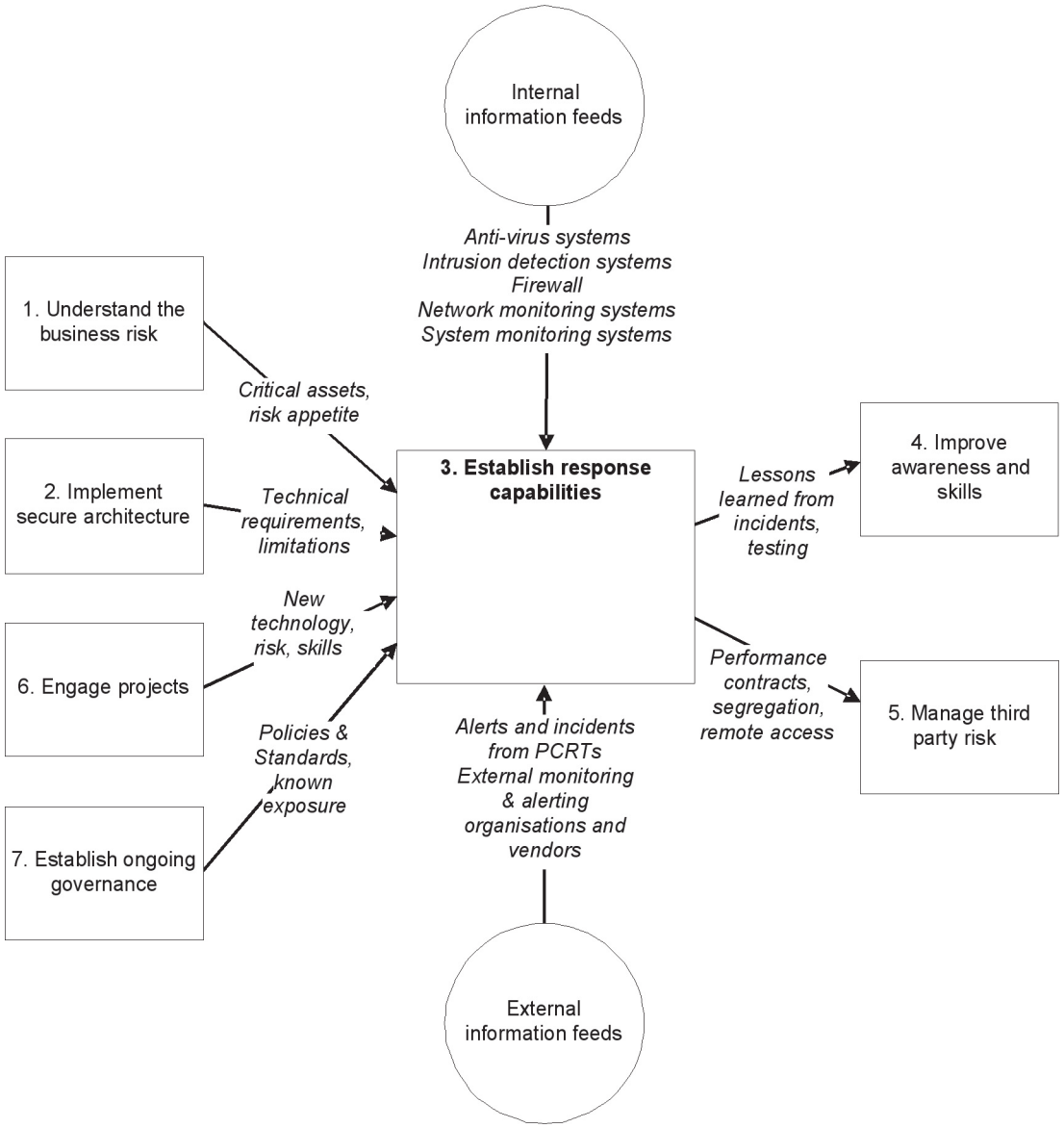

Figure 2 – Where 'Establish response capabilities' fits in the framework

3.2 Rationale

The capability to respond to both alerts and incidents is an important part of a process control security framework. Obtaining management support, determining responsibilities, establishing communication channels, drafting policies, and procedures, identifying pre-defined actions, providing suitable training and exercising the whole process prior to incidents enables a quick, effective and appropriate response which can minimise the business impacts and their cost, possibly avoiding such incidents taking place in the future. Despite these advantages, many organisations do not have comprehensive cyber attack response plans in place to cover process control systems.

3.3 Good practice principles

The relevant good practice principles in the overarching document 'Good Practice Guide Process Control and SCADA Security' are:

- Create a Process Control Security Response Team (PCSRT) to respond to security incidents.
- Ensure that appropriate incident response and business continuity plans are in operation for all process control systems.
- Ensure that all electronic security plans are regularly maintained, rehearsed and tested.
- Establish an early warning system that notifies appropriate personnel of security alerts and incidents.
- Establish processes and procedures to monitor, assess and initiate responses to security alerts and incidents. Possible responses may include: increase vigilance, isolate system, apply patches, or mobilise the PCSRT.
- Ensure all process control security incidents are formally reported and reviewed.
- Lessons learned should be fed back to improve plans and update policy and standards.

The location of the CPNI guide for incident response can be found in Appendix A. The Guide focuses on establishing response plans for incidents such as malware infections or when hackers have compromised systems. Although primarily drafted for traditional IT systems many of the principles embodied within the document are transferable to process control and SCADA systems.

This 'Establish Response Capabilities' guide is aligned with the CPNI First Responders' Guide and covers in more detail some of the proactive areas, such as responding to security alerts and system patching, which are bigger challenges in control system environments than might be in corporate IT systems.

3.4 Good practice guidance

3.4.1 Create a Process Control Security Response Team (PCSRT)

A Process Control Security Response Team (PCSRT) is a core element of an organisation's response capability and provides the foundation for effective monitoring, analysis and managing the response to alerts and incidents. The PCSRT must be involved at every step in the process of monitoring a situation, analysing any changes to the cyber threat and initiating appropriate responses.

A key requirement for a successful PCSRT is to ensure that the right people with the appropriate knowledge and skills are involved. The team can either be part-time or full-time and may be a central resource, a site resource or a combination of these. Membership should be drawn from a variety of sources with representatives from a number of business areas, examples of which include:

- Process control, SCADA, automation teams
- IT security
- IT infrastructure
- Business management
- Operations
- Internal regulators
- Legal department
- Corporate media contact
- Corporate security team.

Organisational considerations

PCSRTs can be structured in a number of ways, either centrally run, i.e. as a Co-ordination Centre (CC), or local site run entities or a combination of both.

In large organisations, it may be possible to have a Coordination Centre (CC) that can monitor and analyse events, advising local sites on appropriate actions and co-ordinating their activities. A CC can provide a better approach to incident response as it is usually ideally placed to share and obtain information from other groups such as business partners, vendors, other Incident Response Teams, law enforcement and infrastructure protection teams such as CPNI.

A CC can also often provide an effective 24/7 operation using fewer resources than a collection of individual local teams. However, a CC also has disadvantages. For example, it may not have enough knowledge of the local sites to fully understand their operational environment or the personalities involved.

The alternative is that of a local site team that might be created using personnel who have a part time incident response role which is performed alongside their normal day to day activities. Local site teams will have extensive knowledge of local issues and operational environments.

In practice, a hybrid approach is often preferable, i.e. a CC sharing information with local teams based at the operational sites. This model leverages the efficiencies of a CC in carrying out day to day monitoring, enabling the local site to concentrate on their normal core activities but responding to incidents or alerts when advised by the centre.

One of the major difficulties in this area, regardless of the preferred operational model, is the availability of personnel with the necessary operational, interpersonal, technical and incident management skills. Significant training may be required before a team can become fully effective.

3.4.2 Establish security response and continuity plans

In many organisations, there is often a variety of response and continuity plans in existence. Such plans include business continuity, disaster recovery, safety, health and environmental incident or other organisational and industry specific emergency plans.

However, it is rare for existing plans to adequately cover the variety of potential threats that face control systems – quite simply the threats, especially from cyber threats, were never really acknowledged when the plans were originally conceived. For example, if a disaster recovery system, installed to protect a control centre from physical incidents, is connected to the same network as the main control centre, then it is likely that a malware incident on the main system would impact on the disaster recovery system potentially rendering it virtually worthless.

It may be possible to include cyber threat incident management within existing plans to save the time and effort but care must be taken to ensure that all the appropriate process control threats are adequately covered and that the various plans interoperate satisfactorily.

There can often be confusion around how incident response, disaster recovery and business continuity planning fits together. **Figure 3** below shows how some of these plans interrelate.

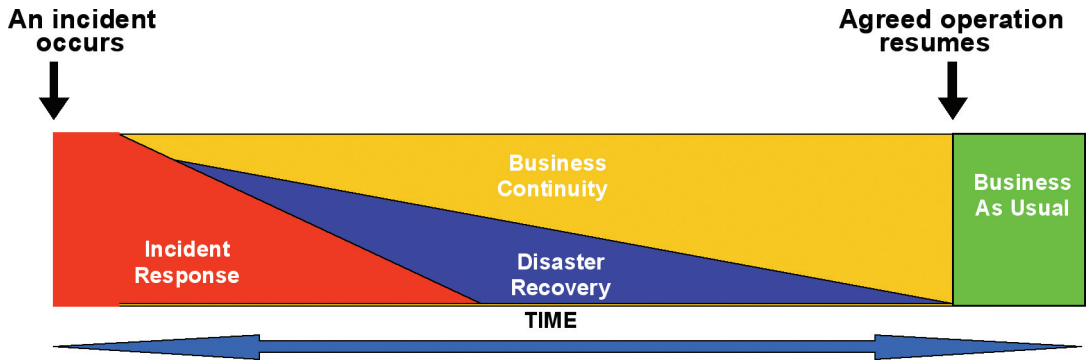

Figure 3 – Different types of response plan

The figure shows how incident response plans focus on the short period of time directly following an incident. Incident response plans are focussed on providing an immediate response to events by implementing immediate actions. As incidents progress, the focus shifts to initiating business continuity (ensuring the business can continue to operate during the incident) and disaster recovery (restoration of lost or damaged data and systems).

In establishing effective response plans for process control systems, there must be a focus on incident response, as digital security events often occur suddenly without notice and require a rapid and effective response in order to avoid incidents or minimise their impact if they cannot be avoided.

3.4.3 Key contents of a incident response plan

Process control security response plans are often quite wide-ranging and must be drafted in accordance with the chosen operational model, e.g. as a CC or local site, however as a minimum they should include:

- Procedures of how to report incidents
- Process to invoke the response plan
- Details of the response team personnel, their deputies, roles and responsibilities and full 24/7 contact details.
- Critical sites, systems and assets
- Predefined procedures to possible scenarios as previously identified (see section 3.4.6)
    - A clear definition of how to identify each scenario
    - A clear action plan in the event of a scenario being identified as in progress
- A clear escalation path, and authorisation requirements for escalation
- Lists of supporting tools available
- Contact information (including both internal and external agencies, companies, law enforcement, vendors etc)
- A clear communication plan
    - How to communicate
    - What to communicate
    - To whom
    - When to communicate and how often
- The criteria to be met in order to close out incidents.

3.4.4 Ensure plans are regularly maintained, rehearsed and tested

Despite careful planning, it is often found that plans and personnel behave differently in real life situations. All personnel should be trained in the execution of the plans which should be regularly tested to ensure that they perform in the manner they were designed.

This topic is covered further in the ‘Improve awareness and skills’ element of the good practice framework.

Plans should be reviewed at least annually and more frequently for critical or high-risk systems. They should be modified following any changes to the threat or protective security requirement, the system itself or organisational structure. Lessons learned during an exercise or following incidents should also be incorporated into the plans.

3.4.5 Establish an early warning system

Having a well defined and rehearsed early warning system will enable organisations to respond rapidly and effectively to security alerts and incidents, minimising their cost and disruption.

Many organisations have response and continuity plans in place but often they are not effective at identifying security incidents, determining the appropriate action and initiating the response plans.

A common problem is not having timely access to appropriate information from internal and external sources on which they can base decisions. Another issue is that they are overwhelmed by a large volume of information that they cannot effectively process. Consequently, they are unsure of the problem and how to react to it.

An example of a high level incident triage process is outlined in Figure 4 which describes three key stages involved in responding to events.

- **Monitor** – collecting information security data from inside and outside the organisation, such as alerts, virus infections, threats, patch notifications, incident notifications and data from network and performance monitoring systems

- **Analyse** – categorisation of the information received from the various sources into different levels and types of potential threat, filtering out the appropriate data for which a response is needed.

- **Respond** – how to respond based on the type and category of threat and the associated risk to the organisation.

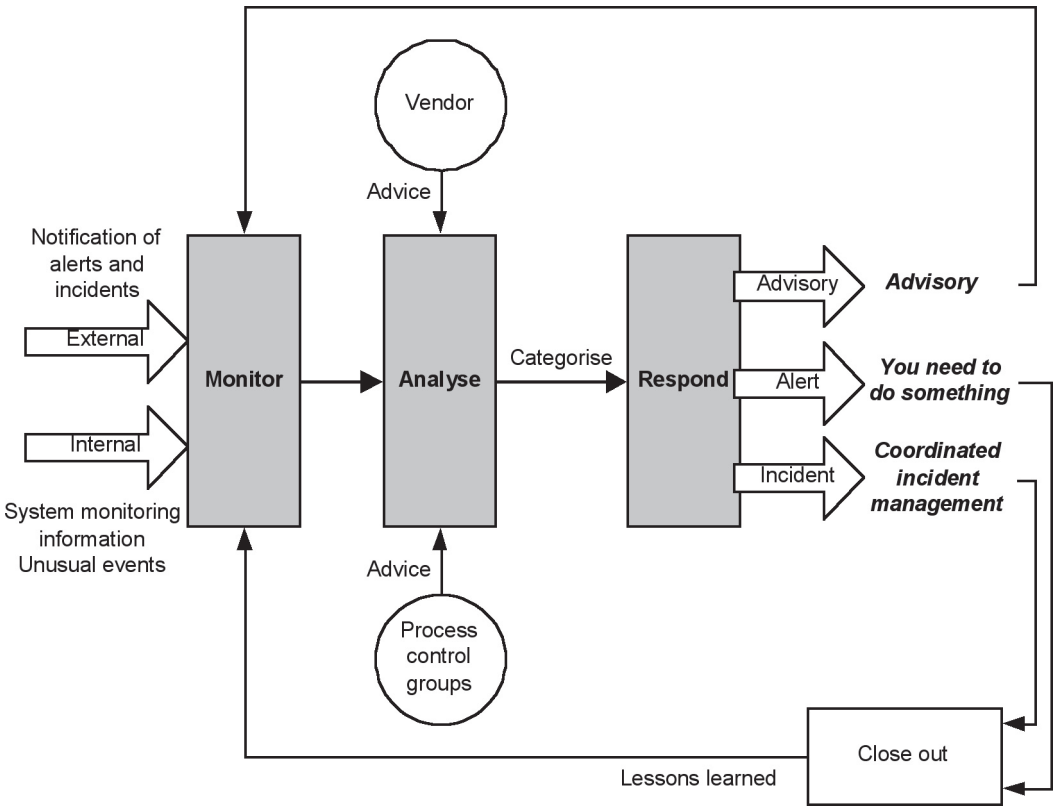

Figure 4 – Process control security response overview

Monitoring stage

The normal state of operations is where both internal and external information feeds are monitored for any relevant events such as security alerts, malware and vulnerability notifications or abnormal system behaviour. A balance needs to be found between trying to process every scrap of information available, which would require a large resource effort, and collecting

enough data such that important alerts or incidents are not missed.

Monitoring should be tailored to the threats applicable to the relevant systems. This can be done by cross-referencing security alerts with the process control systems inventory. There are a number of typical internal and external sources that are generally relevant to most organisations. Some examples are:

Common internal information sources

Examples of internal information sources include:

- Firewall monitoring systems
- Intrusion detection systems
- System and network performance monitoring systems
- Virus and malware reports
- System fault reports
- Helpdesk reports.

Common external information sources

Examples of external information sources include:

- Infrastructure Protection Teams, e.g. CPNI
- Computer Security Incident Response Teams (CSIRTs)
- US-CERT
- CPNI Information Exchanges
- Hardware manufacturers
- Control systems and application software vendors
- Operating system vendors
- Antivirus companies
- External security monitoring organisations (e.g. outsourced firewall and IDS monitoring)
- Technical media
- Newsgroups
- Security forums
- Law Enforcement Agencies

Information from the various monitoring sources may be received in a variety of different forms, e.g. raw system logs, Emails, websites, RSS feeds, pager or even mobile phone text messages. The task of assessing this data can be time consuming so it is worth putting in place processes to filter out superfluous data and present only the important information, preferably in as clear a way as possible.

Some specialist organisations can provide alerting services that are tailored to an organisation's needs, greatly reducing the burden on internal monitoring systems. Unfortunately, this information is often focussed on general IT security topics rather than directly related to process control systems. The information can also be very technical and may need experienced personnel to analyse effectively.

There are a number of information sharing services that can be used both to provide information and to receive information from;

- WARPS
- CPNI information sharing.

References can be found in appendix A.

Analyse stage

Analysing large volumes of system data and internal/external information feeds needs to be conducted quickly and effectively. For example, there is little value in taking ten days to determine that a new worm represents a problem to the organisation as it may have infected systems far sooner!

It is important to have personnel with the right expertise contributing to the analysis of security alerts, incident reports and information feeds. Although control systems are now often based on standard IT technologies, there are differences between the two environments. For example, personnel with networking skills and knowledge of application software will be able to understand the general IT issues but in the process control environment personnel with the relevant knowledge of those systems must also be involved.

Each alert needs to be assessed for the potential impact on the process control systems in use and any appropriate action agreed. The assessment can be complex and any resulting analysis needs to be expressed in a clear and concise manner before being communicated to PCSRT teams. One useful way is to categorise the information based on the threat (Figure 5) e.g.:

- Severe – a current incident or very high threat e.g. worm outbreak on the internet or on the corporate or process control network
- High – high threat vulnerability, e.g. important external activity
- Advisory – low threat vulnerability at present further monitoring is required, e.g. activity on the internet
- Low – little direct threat to the control system, e.g. Email virus where the function is not present on the process control system.

In order to simplify the decision making process it can be useful to have agreed predefined criteria for each category. It should be noted that not all threats will easily fit a predefined criteria. Such threats will need the experienced analysis of IT and process control specialists to interpret the available information and make appropriate decisions.

A detailed discussion of the various threat levels can be found in the US Cert document, reference can be found in appendix A.

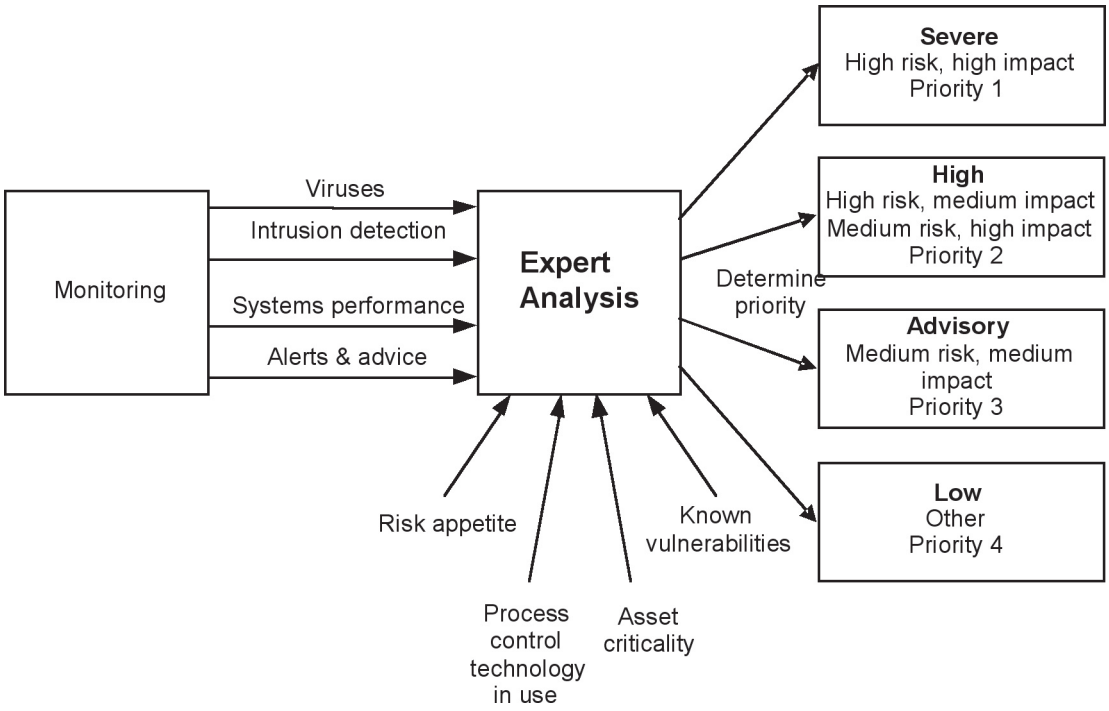

Figure 5 – Categorisation of process control security threat data

In responding to an incident, process control system vendors may have to be included in the analysis process. For example, it may be necessary to seek guidance from a vendor as to whether a particular software patch should be applied or discuss whether a system uses some vulnerable software component.

Many process control system vendors require patches to be tested and accredited prior to deployment on live systems. Some vendors now automatically assess operating system patches as soon as they are released and provide advice on whether to deploy them. Where vendors are not automatically providing this action then a specific request may be needed for such an assessment. Further guidance on patching control systems can be found in section 3.4.6.

Respond stage

This stage is about initiating the appropriate response to an incident in a timely manner. The trigger will normally be the results of the previous analysis stage. Typical situations are:

- Security alert (e.g. advance warning of a possible incident, increased hacker activity or possible malware problem)
- Vulnerability notification (e.g. a vulnerability has been identified or a software patch has been released for a control system)
- Malware infection (e.g. a worm or virus is detected in a control system)
- Hacker infiltration (e.g. a hacker has managed to compromise a control system).

3.4.6 Establish processes and procedures

Examples of what should be considered when preparing a Response plan can be found in the CPNI's First Responders' Guide Policy and Principles the location of this document can be found in appendix A.

The procedures to include in a process control response plan need to take into consideration the operational environment, potential threats, vulnerabilities and experiences from previous incidents. The following are ideas of some procedures that could be included in a response plan:

- Malware infection and removal
- Suspected hacker infiltration
- Denial of service (DoS) attack
- Disconnection of control system from other networks (if possible)
- Reconnection of control system to other networks
- Inability to view status of plant (loss of view)
- Inability to control the plant (loss of control)
- Emergency anti-virus and intrusion detection system signature updates
- Business as usual and emergency security patching processes.
- System backup and restore
- Confirmation of correct system operation (i.e. a procedure for verifying that a system is operating as normal).

The following sections examine considerations for a subset of these procedures.

Security patching

In the past the topic of applying security patches to process control systems was never a significant issue. This was because these systems were based on proprietary technologies or isolated from other systems. Patches were only really required for system upgrades or for fixing bugs. Consequently application of these patches could usually be planned into an orderly installation process.

As most control systems are now based on standard IT technologies and are connected to other systems they run a risk of compromise or infection. Applying protection measures such as firewalls to these systems is an important element of defence. However relying on a single strong layer of defence is no longer considered good practice for protecting process control systems protection and a multi layer 'defence in depth' model is required. A key element in such a model is to ensure that the devices located within the protection perimeter are hardened through a variety of measures – a key one being the application of security patches.

To patch or not to patch – that is the question!

When faced with a security alert or incident a key consideration is whether to deploy security patches or not. This should be largely driven from the risk assessment in the analyse stage. However the application of patches is not risk free – there is a risk that the patch might cause incorrect operation of a system. Also the effort and disruption of taking systems out of production to apply the patches needs to be weighed against the risk of not deploying the

patch. Where possible systems should be designed for ease of patching, for example dual servers so one can be patched while another maintains operations or the provision of test or backup servers where patches can be tested on systems before deployment to the live systems.

In order to provide a consistent approach to system patching and an orderly deployment of the patches the response plan should contain a detailed patching process. In developing this process there are a number of criteria that should be considered:

- What are the systems that might need to be patched (can be obtained from the process control system inventory)?
- What is the patchability of systems?
  - Vendor guidance and requirements
  - N.B. it may not be possible to deploy patches to obsolete technology
- What can be done with systems that can't be patched?
  - Replace or upgrade systems
  - Physically isolate systems
  - Segregate systems (e.g. by placing behind an appropriately configured firewall)
  - Protect system with intrusion prevention systems
- What are the patching priorities?
- In what order should systems be patched?
- How will patches be deployed?
  - Under business as usual situations
  - Emergency patch processes
- What patch deployment and audit tools are available and appropriate?
- What testing is required prior to deployment?
  - Is vendor accreditation required prior to patching systems?
  - Is site assurance testing on test rig or training system possible?
  - Is it possible to patch some systems prior to vendor approval?
- Are there any assurance and deployment tools that could be used to assist the deployment process (N.B. these tools might require vendor accreditation prior to use)?

Further details on general patch management can be found in the CPNI guide, 'Good Practice Guide Patch Management' (see appendix A). This guide is a general document and is not specific to process control and SCADA systems.

System restoration and forensics

Where there has been a compromise of a system (e.g. by malware or a hacker) there is often a difficult decision to make as to whether to restore a system or keep the systems quarantined for further investigation. There is usually a pressing need to restore the systems to an operational state as quickly as possible, which usually involves rebuilding of a system or restoring a system from backups. Unfortunately this usually means that any clues or audit trail left by the attacker would be destroyed and therefore there will be little chance that the perpetrator can be pursued and brought to justice. In this situation the key decision to be made is whether to maintain any audit trails (and possibly delay the restoration of operations) or to restore operations at the expense of being able to pursue the perpetrators. Having spare or redundant systems could enable operations to be restored while the impacted machines could be quarantined for later analysis.

If an organisation is likely to want to pursue perpetrators following an incident then this should be built into the incident response plans to ensure that appropriate systems are quarantined. This topic is a specialist area in itself; for further information refer to the CPNI document, An Introduction to Forensic Readiness Planning, the location of this document can be found in appendix A.

3.4.7 Establish incident reporting

There is a strong tendency for process control security incidents to be kept confidential and for organisations not to disclose incident information to external agencies in order to protect reputation and not to encourage external scrutiny.

However, there are advantages to sharing information about incidents. Sharing such information can allow further investigation by other agencies, the avoidance of similar incidents in other organisations and develop a better understanding of the risks facing control systems.

Any organisations that have experienced process control security incidents are strongly encouraged to share this information (in an appropriate manner e.g. anonymously). CPNI, via CSIRTUK, would like to hear about potential security vulnerabilities, incidents or events, whether in the electronic, physical or personnel security spheres from national infrastructure organisations. This information will be treated as confidential, and if necessary, suitably sanitised to remove particulars that would identify individuals or organisations, for incorporating into generic security advice. The CSIRTUK Help Desk can be contacted via the following email address, csirtuk@cpni.gsi.gov.uk. Sensitive information should not be sent via unencrypted email. Contact the Help Desk for advice about how sensitive information can be sent.

CSIRTUK is a member of the Forum of Incident Response and Security Teams (FIRST) and has contacts with other international Incident Response Teams (IRTs) in order to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing amongst its members and the community at large.

3.4.8 Ensure lessons are learned from incidents

It is important to ensure that following situations where a response to a digital security alert or incident has been required, any lessons or possible improvements to the process are identified and acted upon to ensure continuous improvement of the response processes.

Post incident reviews should be carried out both centrally and locally and could trigger updates to response plans, policy & standards and the enterprise risk profile.

APPENDIX A: DOCUMENT AND WEBSITE REFERENCES USED IN THIS GUIDE

CPNI
www.cpni.gov.uk/

CPNI Good Practice Guides
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

DHS Control Systems Security Program
http://csrp.inl.gov/

DHS Control Systems Security Program Recommended Practices
http://csrp.inl.gov/Recommended_Practices.html

NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

ISA SP99, Manufacturing and Control Systems Security
www.isa.org/mstemplate.cfm?section=home&template=/TaggedPage/getStandards.cfm&MicrositeID=988&CommitteeID=6821

Section 3.4.5

US Cert
www.us-cert.gov/control systems/

WARPS
www.warp.gov.uk/

CPNI Information Sharing
www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx

Control System Cyber Security Self-Assessment Tool (CS2SAT)
www.us-cert.gov/control_systems/pdf/CS2SAT.pdf

Section 3.4.6

Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

An Introduction to Forensic Readiness Planning
www.cpni.gov.uk/docs/re-20050621-00503.pdf

CPNI First Responders' Guide: Policy and Principles
www.cpni.gov.uk/docs/re-20051004-00868.pdf

GENERAL SCADA REFERENCES

BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice
www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Security/Security-Products/BS-78582006/

BS 8470:2006 Secure destruction of confidential material. Code of practice
www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030127562

Best Practice Guide Commercially Available Penetration Testing
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

CPNI First Responders' Guide: Policy and Principles
www.cpni.gov.uk/docs/re-20051004-00868.pdf

CPNI SCADA Good Practice Guides
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

CPNI Information Sharing
www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx

CPNI Personnel Security measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
www.cpni.gov.uk/Docs/re-20060802-00524.pdf

Good Practice Guide on Pre-Employment Screening
www.cpni.gov.uk/Products/bestpractice/3351.aspx

An Introduction to Forensic Readiness Planning
www.cpni.gov.uk/docs/re-20050621-00503.pdf

Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

DHS Control Systems Security Program
http://csrp.inl.gov/

DHS Control Systems Security Program Recommended Practice
http://csrp.inl.gov/Recommended_Practices.html

Guide to Industrial Control Systems (ICS)
http://csrc.nist.gov/publications/PubsDrafts.html

Securing WLANs using 802,11i
http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf

Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdfISA SP99 –

DHS Catalog of Control System Security Requirements
www.dhs.gov

Manufacturing and Control Systems Security
www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

ISO 17799 International Code of Practice for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

ISO 27001 International Specification for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

MU Security Industrial Control (MUSIC) Certification
www.musecurity.com/support/music.html

Control System Cyber Security Self-Assessment Tool (CS2SAT)
www.us-cert.gov/control_systems/pdf/CS2SAT.pdf

Department of Homeland Security Control Systems Security Training
www.us-cert.gov/control_systems/cstraining.html#cyber

Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf

Achilles Certification Program
www.wurldtech.com/index.php

American Gas Association (AGA)
www.aga.org

American Petroleum Institute (API)
www.api.org

Certified Information Systems Auditor (CISA)
www.isaca.org/

Certified Information Systems Security Professional (CISSP)
www.isc2.org/

Global Information Assurance Certification (GIAC)
www.giac.org/

International Council on Large Electric Systems (CIGRE)
www.cigre.org

International Electrotechnical Commission (IEC)
www.iec.ch

Institution of Electrical and Electronics Engineers (IEEE)
www.ieee.org/portal/site

National Institute of Standards and Technology (NIST)
www.nist.gov

NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

Norwegian Oil Industry Association (OLF)
www.olf.no/english

Process Control Security Requirements Forum www.isd.mel.nist.gov/projects/processcontrol/
US Cert
www.us-cert.gov/control_systems/

WARPS
www.warp.gov.uk

ACKNOWLEDGEMENTS

PA and CPNI are grateful for the comments and suggestions received from the SCADA and Control Systems Information Exchange and from other parties involved with CNI protection around the globe during the development of this good practice guidance framework. Contributions have been gratefully received and are too numerous to mention individually here.

About the authors

This document was produced jointly by PA Consulting Group and CPNI.

Centre for the Protection of National Infrastructure
Central Support
PO Box 60628
London
SW1P 9HA
Fax: 0207 233 8182
Email: enquiries@cpni.gov.uk
Web: www.cpni.gov.uk

For further information from CPNI on process control and SCADA security:
Internet: www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

PA Consulting Group
123 Buckingham Palace Road
London
SW1W 9SR
Tel: +44 20 7730 9000
Fax: +44 20 7333 5050
Email: info@paconsulting.com
Web: www.paconsulting.com

For further information from PA Consulting Group on process control and SCADA security:
Email: process_control_security@paconsulting.com
Web: www.paconsulting.com/process_control_security