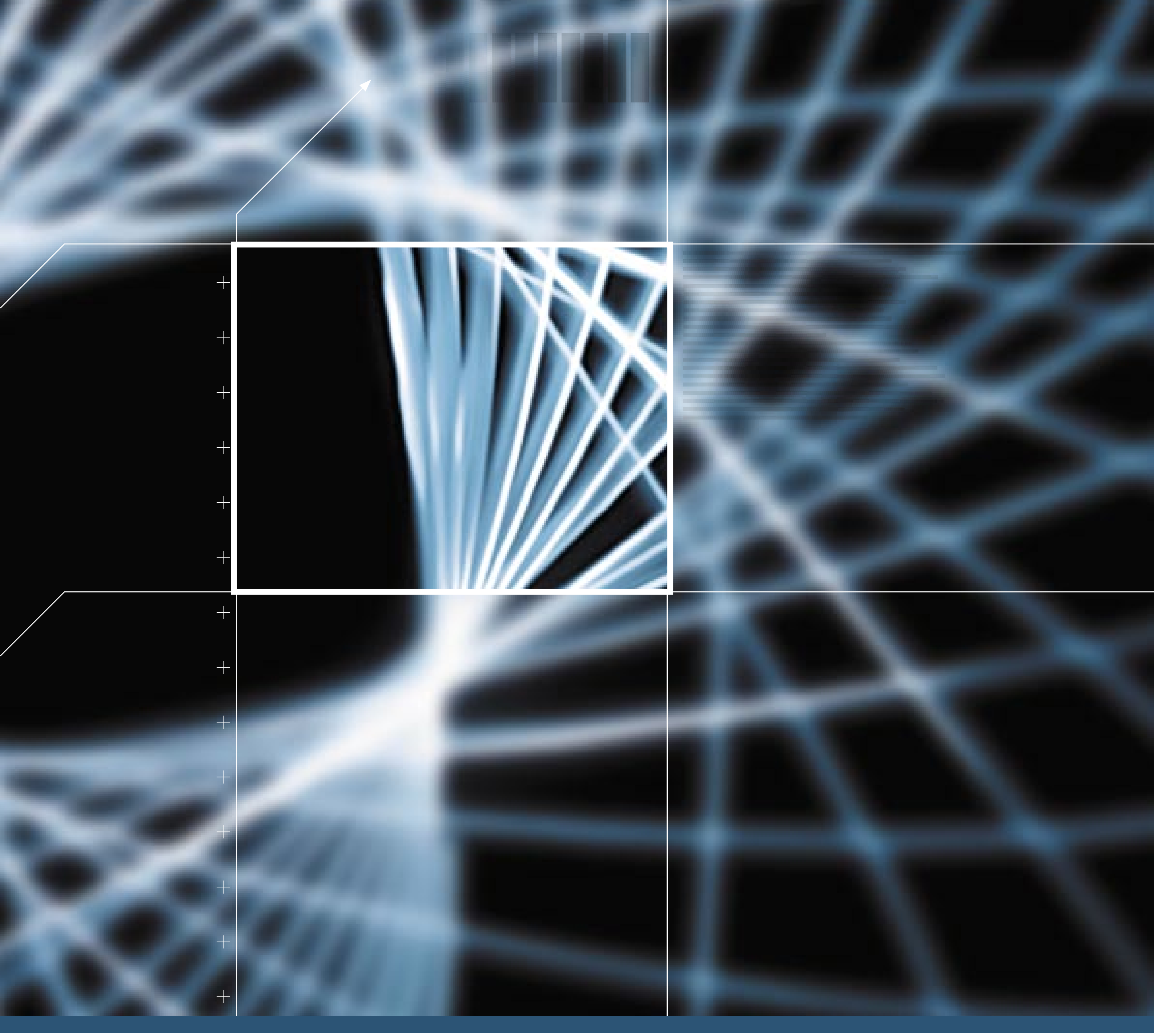

GOOD PRACTICE GUIDE

PROCESS CONTROL AND SCADA SECURITY

GUIDE 4. IMPROVE AWARENESS AND SKILLS

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.

Disclaimer
Reference to any specific commercial product, process or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation or favouring by CPNI or PA Consulting Group. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

CPNI and PA Consulting Group shall also accept no responsibility for any errors or omissions contained within this document. In particular, CPNI and PA Consulting Group shall not be liable for any loss or damage whatsoever, arising from the usage of information contained in this document.

TABLE OF CONTENTS

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.

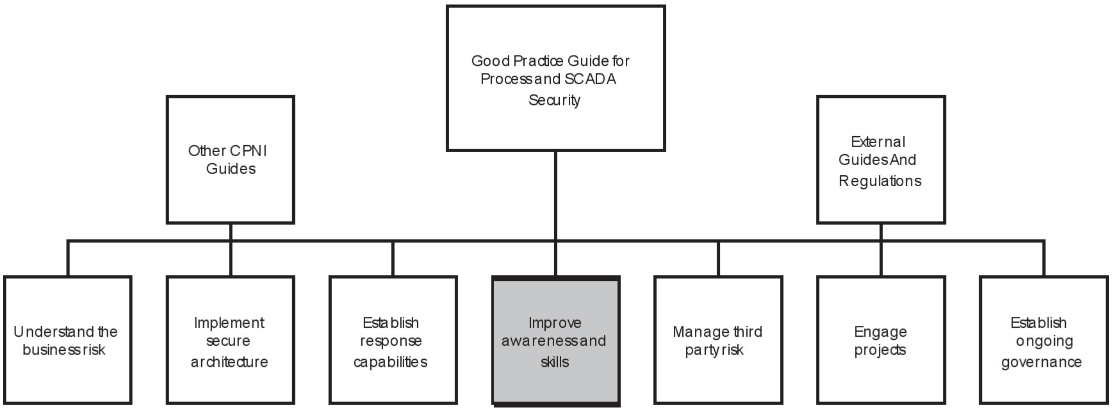
Good Practice Guide for Process and SCADA Security
Other CPNI Guides
External Guides And Regulations
Understand the business risk
Implement secure architecture
Establish response capabilities
Improve awareness and skills
Manage third party risk
Engage projects
Establish ongoing governance

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 **'Improve Awareness and Skills'** guide builds on the foundation provided in the high level good practice guide, and develops the element by looking in detail at each of the key areas and provides generic guidance on improving process control security skills within organisations.

This guide does not provide detailed process control security awareness or training course requirements.

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

2. IMPROVE AWARENESS AND SKILLS SUMMARY

The success of any security framework is ultimately dependent upon the human element – people are the most important resource and potentially the biggest threat to security. In a process control environment process control personnel are often unfamiliar with IT security and IT security personnel are often unfamiliar with process control systems.

Security has traditionally been seen as an issue for the corporate IT environment not the process control environment and traditionally has been the responsibility of the IT department. Additionally a perceived incompatibility of the available security tools and techniques has led to control systems not being adequately secured. The security of process control systems can be improved by increasing awareness, improving skills and by developing a close relationship with IT security personnel.

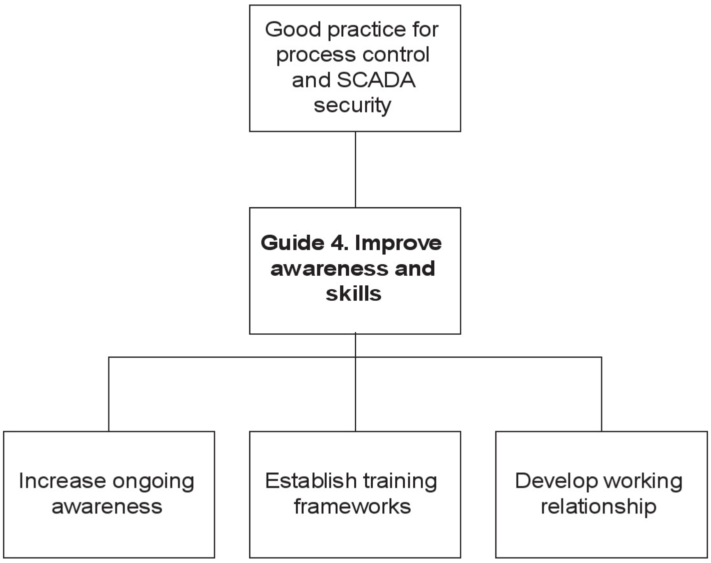
Good practice for process control and SCADA security
Guide 4. Improve awareness and skills
Increase ongoing awareness
Establish training frameworks
Develop working relationship

Figure 2 – Overview of improve awareness and skills

The topic of process control security encompasses a wide audience within an organisation; increasing awareness of this topic highlights the vulnerabilities, threats and risk to these systems, the potential impacts of process control security failures on the business. Awareness programmes should give insights into the technical and procedural solutions that can be deployed to prevent cyber security attacks from succeeding.

Train personnel to give them the appropriate knowledge to adequately secure process control systems - this training should cover a wide technical area, ranging from IT skills through to process control skills. There are few training courses designed for this specific need, so organisations need to develop their own training frameworks to ensure that personnel have the appropriate skills and knowledge to perform their jobs securely.

Awareness and training help develop a close working relationship between process control and IT departments, by providing a common language and processes that can be used to develop an effective process control security programme. Embedding process control security within the organisation is essential for the continued success of any process control security programme.

3. INCREASE ONGOING AWARENESS

3.1 Context of this section within the overall framework

This element of the framework focuses on raising the awareness of process control security topics across a wide range of audiences and builds upon the 'Understand the business risk' and 'Establish ongoing governance' elements of the good practice guide framework.

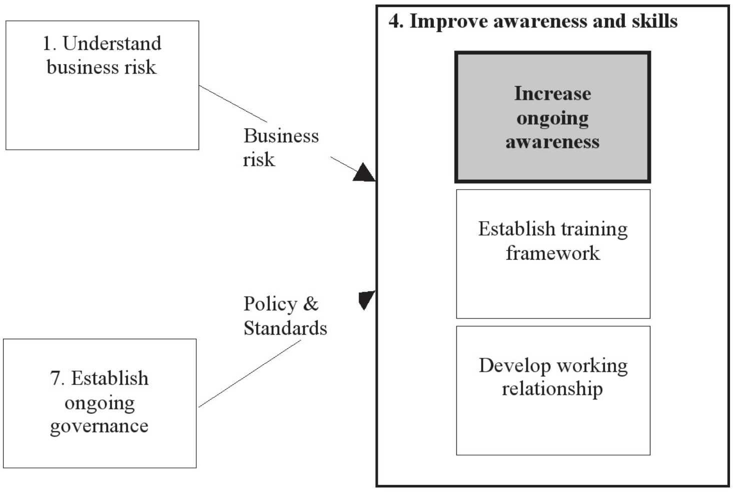
1. Understand business risk
Business risk
Policy & Standards
7. Establish ongoing governance
4. Improve awareness and skills
Increase ongoing awareness
Establish training framework
Develop working relationship

Figure 3 – Where 'Increase ongoing awareness' fits in the framework

3.2 Rationale

Raising awareness is potentially the single most valuable action in the ongoing task of process control security. Raising awareness endeavours to ensure all relevant personnel have sufficient knowledge of process control system security and the potential business impact of lapses in security. Personnel need to know what to do to prevent attacks and what to do in the event of an incident.

3.3 Good practice principles

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

- Engage with senior management to ensure that the business implications of process control security risk are understood and therefore help achieve buy-in for management of this risk
- Establish awareness programmes to increase general security understanding. These programmes will highlight security responsibilities, draw attention to current threats and increase vigilance
- Build the business case to support the process control security programme.

3.4 Good practice guidance

Process control security awareness messages need to be tailored to suit the target audience, To ensure the messages are relevant, received and understood, they should take into account the organisation and its working environment t.

Increasing awareness is not a one-off exercise – it is an ongoing process enabling a cultural change that over time will become embedded within the organisation. There are a number of ways to increase awareness; time should be taken to plan the most appropriate approach to convey these messages to the intended audience. The approach may differ from one organisation to another as the most effective way of raising awareness in an organisation will depend upon the culture of the organisation.

For a process control security programme to be successful there are two key elements relating to awareness that need to be in place, engagement of senior management and establishing an awareness programme. Another key element is that there should be a clearly communicated business case to support the process control security programme.

3.4.1 Engage with senior management

The very process of looking at process control security raises awareness of the issues, however having backing from senior management indicates that the subject is important and people need to take note.

Having the support and engagement from senior management is an essential requirement for being able to get the process control security message out to a wider audience. A champion for process control security can resolve many internal issues ensuring that the message is cascaded through the management levels avoiding delays by getting stakeholder engagement.

In order to engage senior management it may be necessary to demonstrate how important security of control systems is to the business. This may require the development of a business case showing the risks associated with not having a security program and the cost and benefits associated with having one.

Some key benefits from engagement of senior management are:

- understand that the risk exists
- raise the profile of process control security
- message cascade using the management hierarchy and communication channels
- secure appropriate budget for the awareness programme
- understand that some residual risk may remain
- facilitate the removal of internal resource barriers.

3.4.2 Establish awareness programmes

Process control security can be complicated, covering obscure technologies and unfamiliar concepts, consequently the messages need to be crafted into an awareness programme. When determining the awareness message(s) it is important to realise that increasing awareness and embedding is a long-term process not a one off effort – it is a marathon not a sprint!

It is vital that any process control security awareness program is properly planned, a succession of poorly planned and badly executed attempts may hinder process control security programmes. To ensure that an awareness programme is directed and executed well there are a number of areas that need to be considered:

- what is the security awareness objective
- who are the audiences
- understand how communications work within the organisation
- what knowledge already exists in the organisation
- what awareness topics need to be covered
- which awareness methods can be used to convey the message
- how can security awareness be embedded in the organisation
- how well is the message understood.

These areas are described in greater detail in the following paragraphs.

Security awareness objective: having a specific awareness objective or target will focus on the delivery of the key message to the appropriate audiences and allow the success of the programme to be measured. Embedding security into any organisation will take time and the best approach is to focus on the key messages and slowly build up the depth of awareness.

Audience: in identifying the different audiences and recognising that the detail in the message will vary depending upon the audience is vital to the success of a process control security awareness programme. Potential audiences include:

- Process control, automation, SCADA and telemetry engineers
- Business leaders
- Process Control Security Response Team (PCSRT)
- Information security specialists
- Physical security specialists
- Business users
- Risk managers
- Project managers and teams
- Operations personnel
- Health and safety officers
- Support organisations.

Existing communications: before embarking on an awareness-raising programme it is important to understand what communication frameworks and tools are already in place. Understanding how information flows around an organisation, what types of messages are sent and received, which audiences are communicated with, how well communications are planned and received and who has responsibility for communications. Adopting existing mechanisms can ease the task of process control security awareness.

Existing knowledge: an obvious but often overlooked step is to gauge what is already known, perhaps by using a quick survey or poll. This knowledge should be used as a foundation for the awareness topics.

Awareness topics: there are common topics that can be covered in process control security awareness programmes:

- General process control security awareness
- What to look out for and how to react
- Examples of process control security failures and their impacts
- Available policies, standards and solutions
- Updates to existing documents:
    - Policies and standards
    - Vendor guidance
- An explanation and understanding of process control for IT professionals
- An explanation and understanding of IT security for process control professionals.

Awareness methods: there are many ways to raise awareness. The best approach is likely to be a mixture of the below. It is worth considering what would be the best way of getting the awareness message across to your target audiences. The methods include:

- conferences
- email communications
- newsletters
- centralised store for process control security information
- phone calls
- poster campaigns
- videos and DVDs
- websites and webcasts
- workshops
- adding to standard meeting agendas.

Embedding: embedding process control security into an organisation is not likely to happen quickly. It is something that develops over time until process control security becomes an everyday aspect of an organisation. Awareness programmes should be reviewed periodically to ensure that messages are being received, understood and acted upon and so that the process control security programme remains high on an organisation's priorities and is embedded in business as usual operations.

Understanding: It does not matter how good a presentation or message is if it is not understood by the recipients. Feedback is necessary from the recipients to determine if the correct message has being received. Awareness programmes should also be reviewed periodically to ensure that messages are current and acted upon and so that the process control security programme remains high on an organisation's priorities and is embedded in business as usual operations.

3.4.3 Build the business case

It is important to ensure that there is sufficient understanding across the business at different levels of the business case for increasing security of control systems. The key elements of the business case include:

- An overview of the business risk profile (including the potential threats impacts of incidents and vulnerabilities)
- The benefits of improving security of control systems including improved risk profile post improvements (i.e. the business benefit)

- The requirements for a security programme, key activities, resources and costs
- The return on security investment (ROSI).

It may be necessary to carry out this activity at different levels within in an organisation. It may be necessary to construct a low level business case for improvements to a specific site or control system. However in a large organisation it may be necessary to build an overarching business case for the whole organisation. A key advantage of the latter is that work carried out centrally to build the organisation's business case for change will support individual site teams in their activities and reduce the total effort an organisation will have to do to mobilise the security improvement programme.

Further guidance on developing business cases for control systems can be found in the NIST 'Guide to Industrial Control (ICS) Systems' (see appendix A).

4. ESTABLISH TRAINING FRAMEWORKS

4.1 Context of this section within the overall framework

This element of the framework focuses on improving process control security skills in an organisation by establishing a training framework. This builds upon the 'Understand the business risk' and 'Establish ongoing governance' elements of the good practice guide framework.

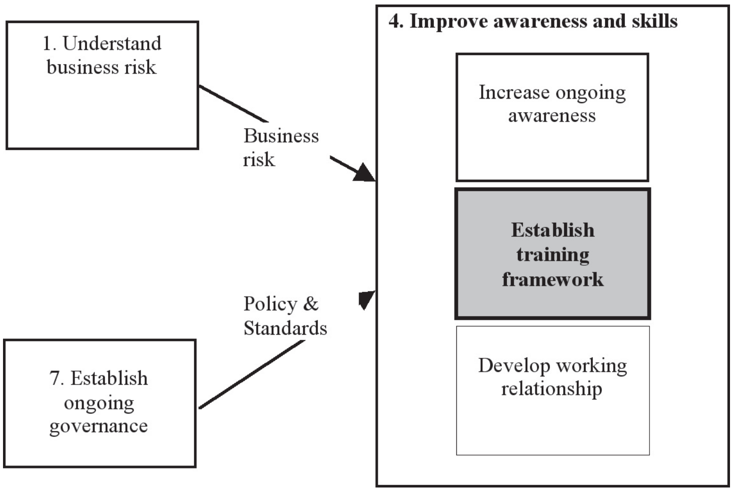
1. Understand business risk
Business risk
Policy & Standards
7. Establish ongoing governance
4. Improve awareness and skills
Increase ongoing awareness
Establish training framework
Develop working relationship

Figure 4 – Where 'Establish training framework' fits in the framework

4.2 Rationale

The concept of process control security is relatively new. Generally, there is a low level of technical understanding and little awareness of the potential business impact. There are few standards available and personnel generally do not have the appropriate skills to carry out both the process control and the security work required. This is not helped by a relative lack of a specific process control security training courses.

4.3 Good practice principles

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

- Coach IT personnel to develop an appreciation and understanding of the process control systems and their operating environments, highlighting the differences between the security of process control systems and IT security

- Develop IT security skills within process control teams and provide appropriate IT support services to these teams.

4.4 Good practice guidance

Most of the differences between the process control and IT operating environments come down to the underlying importance placed on the stability of process control systems. This need drives a conservative risk culture with importance placed on static, robust and repeatable processes and systems.

A training framework should be developed that covers training for the key personnel detailing the level of understanding of an organisation's vulnerabilities, the information and resources that can be accessed to share good practices and approved mitigation measures.

Developing a training plan is similar in many ways to developing an awareness programme and a similar approach can be used. To ensure that the training framework delivers a valued programme there are a number of areas that need to be considered:

- What is the training framework objective?
- Who are the audiences?
- What are the training needs?
- What delivery methods will be used?

These areas are described in greater detail in the following paragraphs.

Training framework objectives: the training framework's objective is not to make everybody a process control security expert but to ensure that personnel have the correct skills for their roles. As well as process control personnel learning about IT security the IT teams need to develop a good understanding of process control systems. The objective of creating a framework is to provide this core understanding so that they can:

- communicate effectively with a shared 'language'
- understand the different operating environments
- transfer sufficient skills to enable process control personnel to implement and comply with good IT security measures applicable to the process control environment
- transfer sufficient skills to enable IT personnel to effectively support process control security requirements.

Identify the audience: from the training framework objective and the analysis of the various audiences, it becomes possible to determine the training needs for each audience. Identifying the audiences helps breakdown the training requirements into a manageable plan, and provide a tool for prioritising what order training should be rolled out to the stakeholders. Examples of the various audiences are:

- Champion of process control security
- Single Point of Authority (SPA)
- Process control, automation, SCADA and telemetry engineers
- IT personnel
- The response team
- The operations team

Training needs: the level of training required will vary depending on the individuals (e.g. a SPA will need to be aware of standards and regulation whereas an individual in charge of firewall rules will need to be technically competent in firewall management).

There are a number of training topics that can be considered for a variety of audiences:

- Policies and standards – the focus will be on the standards and legislation
- Procedures – this details the procedures and how they are related to the policies and standards
- Incident response – this covers what needs to be done in the event of an incident
- Architecture – this covers how the various systems are connected together and configured and will be of a technical nature
- Vendor specific training – this will involve security training specific to a vendor's systems
- Detailed technical training – this usually covers general IT security and can be part of a formal industry recognised accreditation.

Delivery methods: there are comparatively few courses designed specifically for process control security. Of the general IT security courses available, finding which one will provide the appropriate level of understanding can be a difficult and time consuming process. Analysing training needs is a big help in this area and selecting courses run by well-established professional organisations will ensure some of the training needs are met. However they are unlikely to offer the complete package and a mixture of delivery methods is likely to be needed. Typical methods that can be used include:

- **Internal training** – sessions provided internally often provide the most relevant training, as they will deal with organisation specific topics and can give context to knowledge gained externally. However, they can consume a great deal of time and valuable resources in planning and delivery

- **External training courses and approved third party training** – either provided by vendors or security professionals, technical in nature and sometimes difficult to relate back to specific site issues. There are a variety of professional bodies that provide security accreditation such as those listed below (links can be found in Appendix A):

  - Security assurance – Certified Information Systems Auditor (CISA)
  - Security governance – Certified Information Security Manager (CISM)
  - Security management – Certified Information Systems Security Professional (CISSP)
  - Security techniques – Global Information Assurance Certification (GIAC).

- **Computer based and online training and webinars** – can be used for individual and team training at relatively low cost.

- **Conferences and workshops** – attending conferences is a good way to learn about process control security and many industry bodies running conferences often have training workshops as part of the event.

- **Refresher courses** – training is not a one off exercise, courses will need to be taken to ensure personnel remain up to date with changes in threats and technologies and to maintain their skill level.

- **One to one sessions** – this is a valuable tool for key stakeholders, enabling these individuals to be bought up to speed quickly and ensuring the message is understood.

- **Structured training courses** – can either be external or internal and will focus on a specific training topic or objective (e.g. firewall installation and configuration).

- **Self-assessment** – self assessment is a valuable tool that allows an organisation to retain ownership of process control security and measure the success of mitigation plans.

- **Multidisciplinary workshops** – gathering together process control security stakeholders to discuss security improvements enables a wide range of experience and knowledge to be applied to a problem, and can highlight gaps that may require external assistance.

The US Department of Homeland Security provides some web based training resources (see appendix A).

5. DEVELOP WORKING RELATIONSHIP

5.1 Context of this section within the overall framework

This element of the framework focuses on improving process control security skills within the organisation by developing working relationships and embedding process control security within the organisation. This topic builds upon the 'Understand the business risk' and 'Establish ongoing governance' framework good practice elements and upon the 'Increase ongoing awareness' and 'Establish training framework' elements within this document.

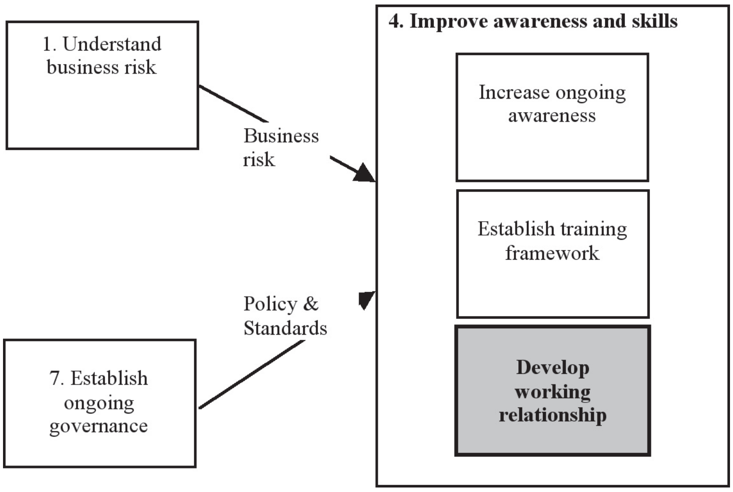
1. Understand business risk
Business risk
4. Improve awareness and skills
Increase ongoing awareness
Establish training framework
Policy & Standards
7. Establish ongoing governance
Develop working relationship

Figure 5 – Where 'Develop working relationship' fits in the framework

5.2 Rationale

As the process control and IT world converge the two communities need to work closer together to protect both environments in an efficient manner providing better integrated solutions, improving staff utilisation and producing cost savings.

5.3 Good practice principles

The relevant good practice principle in the overarching document 'Good Practice Guide Process Control and SCADA Security', is:

- To establish links between IT security and process control teams in order to build working relationships, share skills, and facilitate knowledge transfer.

5.4 Good practice guidance

Process control and IT have traditionally been two different fields. The recent trend of technology convergence and the requirement to connect the two environments has highlighted the need for improved relationships between IT and process control departments. It is important for both teams to be aware of each environment so that working relationships and shared understanding can be successfully developed.

Process control personnel can develop skills around IT applications, infrastructure and security. Similarly IT personnel can develop core process control skills including business critical change control and testing practices.

By developing a two way relationship a number of mutual benefits that can be realised:

- Increased knowledge transfer
- Access to a wider security skill base
- Access to a wider process control skill base
- Better understanding of security protection
- An opportunity to share best practices
- Lower cost security solutions
- More efficient working practices
- Faster project delivery.

Some simple actions that can be taken to help reinforce good working relations are:

- IT representation on the Process Control Security Response Team (PSCRT)
- Establishing regular meetings to discuss security developments and progress
- Inviting IT representatives to process control change boards.
- Extending distribution lists to include appropriate IT contacts
- Establishing a mentoring scheme
- Have process control representation on the organisation security team
- Job share – IT and process control staff cross-training and covering each other's roles
- Combined project teams.

In many organisations the IT functions can provide a range of services to the organisation. By developing a close relationship it can be possible to identify IT solutions that can be used in the process control environment, either directly (with minimal tailoring) or by modifying the configuration for the process control environment. Examples of services that may be good candidates for provision by IT include:

- Anti-virus
- Firewall management and monitoring
- Network system monitoring
- Remote access management
- Incident and alert response
- Security training and awareness
- Ongoing assurance management.

APPENDIX A: DOCUMENT AND WEBSITE REFERENCES USED IN THIS GUIDE

Section 3.4.1

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

Section 3.4.3

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

Section 4.4

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/

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

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