CESG

CPNI
Centre for the Protection of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

IMPROVE AWARENESS AND SKILLS

A GOOD PRACTICE GUIDE

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, CESG or PA Consulting Group. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes. The content of this document is based on information available as at the date of publication.

The case study although fictitious is based on the experiences of PA Consulting Group through their work with companies in ICS industries. Any similarities are strictly coincidental and are not based on any one specific company.

This is general guidance only and is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate specialist advice.

To the fullest extent permitted by law, CPNI, CESG and PA Consulting Group and their employees and advisers accept no responsibility for any errors or omissions contained within this document. In particular, to the fullest extent permitted by law, CPNI, CESG and PA Consulting Group and their employees and advisers shall not be liable for any loss or damage whatsoever, arising from any error or omission in this document, or from any person or organisation acting or refraining from acting upon or otherwise using the information contained in this document.

Copyright

Corporate Headquarters:

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

Version no: Final v1.0

Prepared by: PA Consulting Group Document reference:

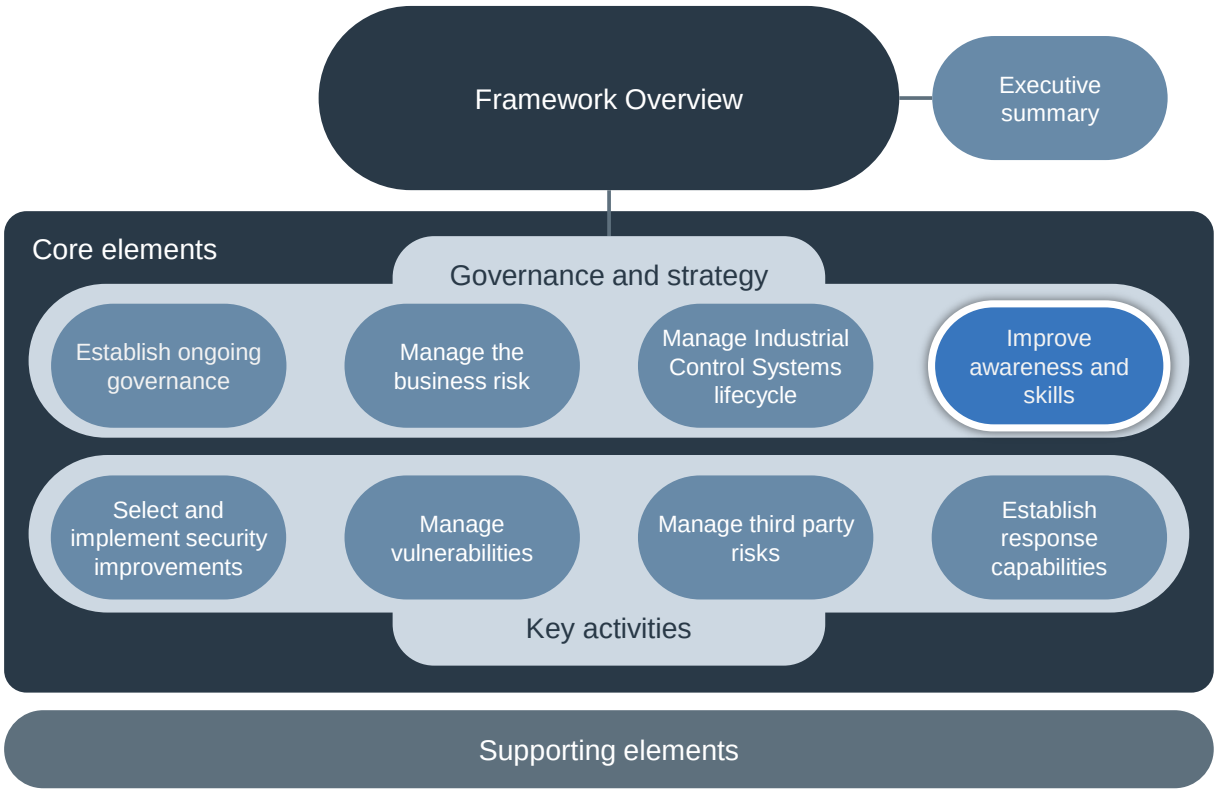
CONTENTS

1 INTRODUCTION

1.1 Framework context

The Security for Industrial Control Systems (SICS) Framework provides organisations with good practice guidance for securing Industrial Control Systems (ICS). This framework consists of a good practice guide Framework Overview, which describes eight core elements at a high level. This is supported by eight good practice guides, one for each core element and which provide more detailed guidance on implementation. Additional supporting elements of the framework provide guidance on specific topics. The framework, core elements and supporting elements are shown in Figure 1.

Figure 1 - Where this element fits in the SICS Framework



1.2 Improve awareness and skills – summary

The objective of this guide is:

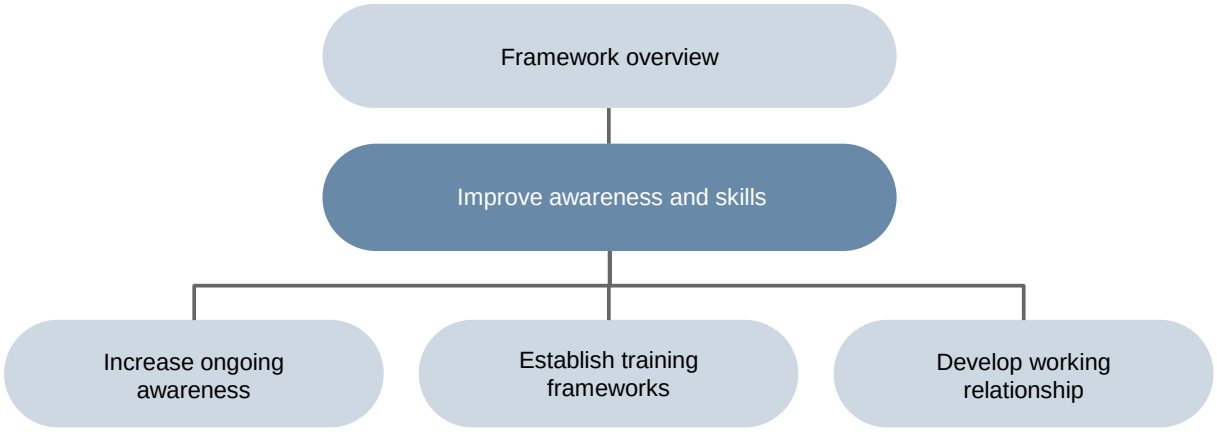
- To increase ICS security awareness throughout the organisation and to ensure that all personnel have the appropriate knowledge and skills required to fulfil their role.

The success of any security framework is ultimately dependent upon the human element – people are both the most important resource and potentially the biggest threat to security. The challenge is that in an ICS environment personnel are often unfamiliar with digital security concepts and IT security personnel are often unfamiliar with ICS. One reason for this is that security has traditionally been seen as an issue for the enterprise IT environment and not the ICS environment and so has been the responsibility of the IT department.

A further problem arises because limited compatibility between some of the available security tools and techniques has meant control systems may not be adequately protected.

The security of ICS can be improved by increasing awareness, improving skills through training frameworks, and by developing a close relationship with IT security personnel. The three good practice principles are shown in Figure 2.

Figure 2 – Good practice principles to improve awareness and skills



Embedding ICS security knowledge and tasks is essential for the continued success of any ICS security programme and there needs to be recognition that the topic is relevant to a wide audience within an organisation. Programmes to increase awareness should highlight the vulnerabilities, threats and risk to ICS, as well as the potential impacts of security failures on the business.

Awareness programmes should also provide insights into the technical and procedural solutions that can be deployed to prevent cyber security attacks from succeeding.

Personnel, including from third parties, should be trained to give them the appropriate level of knowledge to understand the risks and adequately protect the ICS environment. The training should cover technical areas (IT and ICS), policies, processes and procedures. There are an increasing number of training courses designed for these specific areas and organisations should select courses that suit their own training strategy.

Awareness and training can also help develop a close working relationship between ICS and IT departments, and provide a common language and processes that can be used to develop an effective ICS security programme.

2 INCREASE ONGOING AWARENESS

Raising awareness and training is potentially the most valuable action in the ongoing task of ICS security. It endeavours to ensure all relevant personnel have sufficient knowledge to achieve good ICS security and reduces the potential of a business impact due to lapses in security.

Personnel need to know what to do to prevent successful attacks and what to do in the event of a security event or incident. Providing information about these threats should take into account the nature of the organisation and its working environment to ensure the messages are relevant, and received and understood by the appropriate people.

Increasing awareness is not a one-off exercise. It is an ongoing process enabling a cultural change that, over time, should become embedded within the organisation. The approach may differ from one organisation to another and is likely to reflect its culture.

For ICS security programmes to be successful there should be engagement from senior management, the establishment of an awareness programme, and a clearly communicated supporting business case. ICS security awareness should not be seen as an isolated activity that only applies to engineering and maintenance disciplines but should be integrated with more general enterprise security awareness activities.

The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

- **Engage** with senior management to ensure that the business implications of ICS security risks are understood and therefore help achieve buy-in for management of these risks.
- **Establish** awareness programmes to increase general security understanding. These programmes should highlight security responsibilities, draw attention to current threats and increase vigilance.
- **Communicate** the business case to explain the need for the ICS security programme.

2.1 Engage with senior management

The very act of looking at ICS security raises awareness of the subject, while having visible support from senior management highlights its importance.

This support and engagement is an essential element in getting the ICS security message to a wider audience. A senior ICS security champion with the necessary level of authority and recognition can resolve many internal issues. They can also ensure that the security message is cascaded through the management levels avoiding delays that might occur without this kind of senior stakeholder engagement.

The role of an ICS security champion may come with or without formal accountability for the cyber security of the ICS assets.

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

Further guidance about ICS security which can support business case development can be found in the NIST 'Guide to Industrial Control (ICS) Systems'[1].

Some key benefits from engagement of senior management are:

- Understanding that the risk exists
- Agreeing the risk appetite for the organisation
- Raising the profile of ICS security
- A message cascade using the management hierarchy and communication channels
- Securing an appropriate budget for the awareness programme
- Understanding that some residual risk may remain
- Facilitating the removal of internal resource barriers.

2.2 Establish awareness programmes

ICS security can be complicated, covering both bespoke technologies and unfamiliar concepts. As a consequence, messages need to be carefully crafted into a targeted awareness programme.

When determining the awareness message, it is also important to realise that increasing awareness and embedding of knowledge is a long-term process and not a one off effort.

It is vital that any ICS security communication programme is properly planned. To ensure that an awareness programme is directed and executed in the best possible way, there are a number of things that need to be considered:

- What is the objective behind security awareness?
- Who is the audience?
- What understanding is there of 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 below:

Security awareness objective: having a specific awareness objective or target should focus 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 may take time and the best approach is to focus on getting the key messages across and slowly build up the depth of awareness.

Audience: identifying the different audiences and recognising that the detail in the message may then need to vary is vital to the success of ICS security awareness programmes. The potential audience should cover everyone with access to ICS and enterprise IT systems.

Existing communications: before embarking on an awareness raising programme it is important to understand what communication frameworks and tools are already in place. The organisation needs to understand:

[1] http://csrc.nist.gov/publications/PubsSPs.html

- How information flows around its constituent parts?
- What types of messages are sent and received?
- Which audiences are communicated with?
- How well communications are planned and received?
- Who has responsibility for communications?

Adopting existing mechanisms can ease the task of ICS security awareness. In-house communication teams can provide access and help in navigating communications channels.

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 ICS security awareness programmes:

- General ICS security awareness
- Responsibilities for ICS security
- What to look out for and how to react
- Examples of ICS security failures and their impacts
- Available policies, standards and solutions
- Updates to existing documents:
  - Policies and standards
  - Vendor guidance
- An explanation and understanding of ICS for IT professionals
- An explanation and understanding of IT security for ICS professionals
- Management of sensitive information by organisations and their third parties.

It is important that the content of these topics is maintained and kept up to date with current developments within ICS security.

Awareness methods: there are many ways to raise awareness. The best approach is likely to be a mixture of the activities below that best meet the needs of the target audiences. The methods include:

- Conferences
- E-mail communications
- Newsletters
- Centralised store for ICS security information
- Phone calls
- Poster campaigns
- Videos and DVDs
- Websites and webcasts
- Workshops
- E-Learning modules
- Adding to standard meeting agendas.

Embedding: embedding ICS security into an organisation is not likely to happen overnight and is something that develops over time. Its introduction can be improved by its inclusion in work instructions and method statements until the point is reached where ICS security becomes an everyday aspect of an organisation. Awareness programmes should be reviewed periodically to ensure that messages are being received and acted upon. It is important that the ICS security programme remains high on the organisation's priorities list to facilitate it being embedding into business as usual.

Understanding: It does not matter how good a presentation or message is if it is not understood by the recipients. It is necessary to get feedback to determine if the correct message has been received and that it remains current.

2.3 Communicate the business case

It is important to ensure that there is sufficient understanding of the need to increase the security of ICS by communicating the business case widely. The key elements of a business case are described in SICS Framework element 'Establish ongoing governance'.

The communication should articulate the case for different stakeholders to secure their buy-in and adherence to the programme, and set out the timescales for realising the security benefits. This should cover:

- **Why** security is important by highlighting the potential threats and impacts on the organisation
- **How** this can be improved through the rolling out of a security programme and the involvement of all stakeholders
- **What** are the benefits that this security programme should have on managing the risks but also potentially as an enabler for business improvements?

Further guidance on the subject of ICS security, which can support business case development can be found in the NIST 'Guide to Industrial Control (ICS) Systems'[2].

[2] http://csrc.nist.gov/publications/PubsSPs.html

3 ESTABLISH TRAINING FRAMEWORKS

ICS security is still a relatively new concept when compared to IT security. Generally there is now a better understanding and awareness of the potential impact on the business from inadequate ICS security. However, even with the growing number of ICS security standards and training courses, there is still a skills shortage of specialists with knowledge of both security and ICS.

Most of the differences between the ICS and enterprise IT operating environments relate to the underlying importance placed on the stability (availability, integrity and safety) of ICS. This need drives a conservative risk culture with greater importance placed on static, robust and repeatable processes and systems.

The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

- Coach IT personnel to develop an appreciation and understanding of the ICS and their operating environments, highlighting the differences and similarities between the security of ICS and enterprise IT systems
- Develop IT security skills within ICS teams and provide appropriate IT support services to these teams.

3.1 Coach and develop personnel

A training framework should be developed for key personnel. This should detail the organisation's vulnerabilities, the information and resources that can be accessed to share good practices, and approved mitigation measures. This security training framework should be managed according to the organisation's existing HR policies and procedures for people development, skills management, and training planning. This ensures that the security aspects of training are embedded into existing business processes.

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 an effective programme, there are a number of areas that need to be considered:

- What is the training framework objective?
- Who is the audience?
- What are the training needs?
- What delivery methods should be used?

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

3.2 Define training framework objectives

The training framework's objective should not be to make everybody an ICS security expert, but to ensure that personnel have the correct skills for their roles. As well as ICS personnel learning about IT security, the IT teams need to develop a good understanding of ICS. If the organisation has an existing skills management process, security could be addressed as part of it. The objective of creating a framework is to provide this core understanding so that all those involved can:

- Communicate effectively with a shared 'language'
- Understand the different operating environments
- Transfer sufficient skills to enable ICS personnel to implement and comply with good IT security measures applicable to the ICS environment
- Transfer sufficient skills to enable IT personnel to effectively support ICS security requirements.

3.3 Identify the audience

The training framework objective and the analysis of the various audiences (both internal and external) makes it possible to determine the training needs for each audience. This helps breakdown the training requirements into a manageable plan, and provides a tool for prioritising the order in which it should be rolled out to the stakeholders. This should be closely linked to any existing people development process. This could provide a proven framework for managing and balancing the needs of the organisation in terms of skills and the aspirations of each individual. Examples of the various audiences are:

- Champion / Lead for ICS security
- Single Point of Authority (SPA)
- ICS, automation, SCADA and telemetry engineers
- ICS Peer Groups (organisations distributed over multiple locations)
- IT personnel
- The ICS Security Response Team (ICS SRT)
- The operations team

3.4 Tailor training needs

The level of training required may vary depending on the individuals (e.g. a SPA will need to be aware of standards and regulations 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 sector and cross-sector standards and legislation
- **Procedures** – details of the procedures and how they are related to the policies and standards
- **General cyber awareness** – highlight the different threats that can affect systems and how they can be introduced e.g. USBs, other removable media and e-mails
- **Incident response** – what needs to be done in the event of an incident
- **Architecture** – how the various systems are connected together and configured, and will be of a technical nature
- **Vendor specific training** – security training specific to vendors' systems
- **Detailed technical training** – usually covers general IT security and can be part of a formal industry recognised accreditation
- **Threat, vulnerability and incident trends** – sector and cross-sector.

3.5 Deliver the training

There are comparatively few courses designed specifically for ICS 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 and selecting courses run by well-established professional organisations will ensure some of the requirements 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, their planning and delivery can consume a great deal of time and valuable resources.
- **Certification and external training courses** – either provided by vendors or security professionals, or training institutes. There are a variety of professional bodies that provide security courses often leading to certification such as those listed below:
  - ICS Security Awareness for Practitioners Course, ICS Security Awareness for Managers Course, ICS Incident Response Course - CPNI[3]
  - Global Industrial Cyber Security Professional (GICSP) – GIAC[4]
  - CESG Certified Professionals (CCP) – CESG[5]
  - Advanced SCADA Security Red / Blue Team – DHS Idaho National Laboratory (INL)[6]
  - Certified SCADA Security Architect (CSSA) – IACRB[7]
  - Certified Information Systems Security Professional (CISSP) – ISC2[8].
- **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 ICS 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, and courses will be needed to ensure personnel remain up to date with changes in threats and technologies and maintain their skill level.
- **One to one sessions** – these are 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 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 ICS security and measure the success of mitigation plans.
- **Multidisciplinary workshops** – gathering together ICS 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 to support this work.

[3] http://www.cpni.gov.uk/Contact-us/

[4] http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

[5] http://www.cesg.gov.uk/awarenesstraining/certified-professionals/Pages/index.aspx

[6] http://www.inl.gov/scada/training/index.shtml

[7] http://www.iacertification.org/cssa_certified_scada_security_architect.html

[8] https://www.isc2.org/cissp/default.aspx

4 DEVELOP WORKING RELATIONSHIP

As the ICS and enterprise IT world converge, the two communities need to work closer together to protect both environments in an efficient manner. This should lead to better integrated solutions, improved staff utilisation and cost savings.

The relevant good practice in the overarching document 'Security for Industrial Control Systems – Framework Overview' is:

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

4.1 Establish links between IT security and ICS teams

ICS and IT have traditionally been two different fields. However, the trend of technology convergence and the requirement to connect the two environments has highlighted the need for improved relationships between enterprise IT and ICS departments. It is important for both teams to be aware of each other's environment so that working relationships and shared understanding can be successfully developed.

ICS personnel can develop skills around IT applications, infrastructure and security. Similarly IT personnel can develop core ICS 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 ICS 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 relationships are:

- IT representation in the ICS Security Governance group
- IT representation on the ICS Security Response Team (ICS SRT)
- Establishing regular meetings to discuss security developments and progress
- Inviting IT representatives to ICS change boards

- Extending distribution lists to include appropriate IT contacts
- Establishing a mentoring scheme
- Having ICS representation on the organisation security team
- Job share – IT and ICS staff cross-training and covering each other's roles
- Combined project teams.

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

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

Those principles already presented in the SICS Framework remain valid and are all the more relevant as the convergence between enterprise IT and ICS continues and progresses. This is particularly true with the successful wider adoption of some IT security solutions in ICS environments. Until a few years ago, many of these solutions (e.g. IDS, patching and malware protection) were considered ill adapted to the specific constraints of ICS environments. This has now changed as technology vendors develop solutions which are more compatible with modern security measures, and the implementation of new processes (e.g. accreditation / approval of patches by ICS vendors). This has also lead to an increase in security awareness and skills in the ICS community.

5 CASE STUDY: MAJOR OIL & GAS

5.1 Major Oil & Gas

Major Oil & Gas is a multinational organisation active in every area of the oil and gas industry including exploration, production, refining, distribution, petrochemicals and trading.

In recent months there have been several reported breaches of security in the control room at one of their refineries. As yet there has been no known adverse impact resulting from these breaches. The breaches have included the charging of smartphones via the USB port of the Human Machine Interface (HMI), downloading of music files, and leaving server racks and cabinets unlocked. Following an investigation it was found that these incidents are largely due to a lack of awareness of how practices that are normal in everyday home life can have a negative impact on ICS security.

5.2 Making the case

The issue was brought to the attention of the organisation's Chief Information Security Officer (CISO). It was explained that it had become clear that the increase of reported security breaches was due to those using ICS not having an adequate understanding of its security needs. Even after the reports were followed up, security breaches were still occurring with the typical explanation being that those involved did not see they were doing anything wrong.

It was proposed that a training and awareness programme be rolled out across the organisation to increase general security understanding and highlight that ICS security is everyone's responsibility. The benefit would be a reduction of avoidable ICS security breaches.

It was felt that there was also a lack of ICS knowledge amongst IT personnel. This had led to past situations where the IT department had proposed solutions to the ICS engineers that were wholly unworkable in the ICS environment. These solutions were largely based on traditional IT concepts and in some cases had led to by-passing of security controls in order to be able to carry out key business activities.

The CISO recognised the severity of the issue and that the organisation had been lucky that the security breaches had not resulted in a full scale incident. With the buy-in of the CISO, it was agreed to roll out an awareness and training campaign across the organisation to reinforce the message of ICS security.

5.3 Improving awareness and skills

A training framework was created with the objective of increasing the awareness of ICS security among all those involved. This would help to instil a focus on ICS security throughout their day to day roles. The key groups identified were:

- ICS engineers

- IT personnel
- Operators
- Leadership.

A pilot scheme comprising an eLearning package and briefing packs was rolled out at the refinery. Feedback and comments were collected and incorporated into later revisions. Following the successful pilot, the full framework was implemented across the organisation and comprised the following:

- **Awareness:**
  - **eLearning:** introduced the concepts of cyber security to ICS engineers and concepts of ICS to IT personnel
  - **Briefing packs:** provided individuals with additional detailed information to supplement the topics outlined in the eLearning package
  - **Webinars:** provided employees working on other sites with an opportunity to benefit from interaction with key members of the ICS security team
  - **Cross organisation awareness:** tailored to different parts of the organisation to focus on topics specific to them
  - **Dedicated internal conference:** keynote presentation by the CISO to highlight the importance of the topic. Internal and external guest speakers provided real-life experience and insight
- **Training:**
  - **Incident exercise:** highlighted not only what could go wrong but how to respond to it. Also helped to increase the awareness of ICS as the exercise brought in representation from different areas of the business
  - **2 day training course:** built on the eLearning to provide further details and exercises. Classroom based training comprised of IT personnel and ICS engineers to enhance their ICS security knowledge and to allow for the sharing of experiences and the forming of working relationships.

Training material was reviewed on a regular basis to ensure that topics remained relevant and any examples used were current.

5.4 Benefitting from working relationships

As a direct result of the awareness programme the company saw a dramatic drop in reported ICS security incidents in the control room.

Several months after the implementation of the training framework, it was identified by an ICS engineer that a planned project to allow a vendor to remotely access the ICS network for maintenance had not considered the security implications. This was brought to the attention of the project team responsible for this work and through discussion with the IT teams and ICS engineers, a solution was developed to allow secure access through a DMZ jump host and requiring a time limited authentication token.

ACKNOWLEDGEMENTS

PA are grateful for the support and input from CPNI, CESG, the ICS community and those involved with CNI protection 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

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 Industrial Control Systems security:

Email: IndustrialCyberSecurity@paconsulting.com

Web: http://www.paconsulting.com/industries/energy/energy-and-water-cyber-security/