CESG

CPNI
Centre for the Protection of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

EXECUTIVE SUMMARY

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:

EXECUTIVE SUMMARY

Why is the guidance needed?

Major industries and critical national infrastructure are increasingly reliant on modern Industrial Control Systems (ICS) for their core operations. Modern control systems are constructed from commercial off the shelf technologies similar to those used in the IT domain. While this reduces the time and cost of system development and ongoing maintenance, the use of this technology has introduced everyday IT security risks in to the ICS domain.

The fundamental difference between a security incident in the IT domain and the ICS domain lies in the potential impact. The impact of an ICS incident can be far greater, causing not only disruption to business operations and services but also potential damage and destruction of equipment, and injury to people. These systems are critical and therefore are required to be trustworthy and resilient not just operationally but from a security perspective too.

In the past, ICS security was mostly seen as an afterthought and this has led to many of the issues we face today. Although some of these could be resolved by applying standard IT solutions, many remain unresolved due to the particular constraints of ICS. Only by recognising these constraints and implementing industry good practice developed through practical experience can security be improved.

What's changed in ICS security?

Convergence

Businesses have changed the way they operate and are now demanding more from ICS to deliver operational improvements through convergence with the IT domain. As a result, these once separate domains are becoming increasingly connected so they can take advantage of new technologies and live operational data. At the same time, businesses are increasingly reliant on vendors and service providers, leading to a more integrated value chain that requires third party access to an organisation's ICS networks and associated systems. This connectivity is enabling initiatives such as Smart Grid, Digital Oilfield, and smart asset management in the water industry however the security challenges this integration brings need to be considered and managed throughout the lifecycle of an ICS.

Increase in threat

The threat environment that ICS operate in today has changed significantly in a relatively short space of time. Prior to 2010, ICS security was not on the agenda of most businesses but that changed later

that year with the discovery of Stuxnet[1] that specifically targeted ICS. Stuxnet highlighted to the world how vulnerable ICS were and what the impact could be, however it was not till the discovery of Havex[2] and BlackEnergy[3] in 2014 that it became clear that businesses of all sizes were potential targets.

Building on experience

Over the past few years, many lessons have been learnt in dealing with the security of ICS that can be drawn on by all to drive improvements. In the past too much reliance was placed on technical controls which, although they have advanced in response to an ever evolving threat environment, still only represent one of the areas that need addressing. However, more recently there has been a gradual but positive shift in how companies approach security as they take a more holistic view encompassing technology, procedures and people.

Organisations also need to ensure they have access to people with the right level of awareness and skills so that people become their greatest security asset, as those without those skills may be the weakest link. All this means that managing ICS security should reflect a wider perspective that looks beyond technical controls where security is managed as part of the lifecycle of the ICS.

The SICS Framework

This framework is primarily intended for those who are directly responsible for securing ICS, whether they are looking to establish a new programme or complement one that already exists. It can assist ICS professionals in improving their knowledge of security and can provide insight into the ICS environment to IT professionals. Further to this, the guidance can inform the organisation's leadership about the rationale for establishing an ICS security capability and the potential activities involved in securing assets.

The framework is also useful as a point of reference for the wider group of ICS stakeholders who do not have direct responsibility for security but have a vested interest in it or who could have an impact on ICS security. This can include procurement staff (who can manage security requirements in contracts) and project managers (to help them understand the need to address security early in the design process). It can also be used by Lead Government Departments (LGDs) who have a responsibility for understanding how to measure the trustworthiness of ICS that underpin or directly provide critical services.

What is the SICS Framework?

The Security for Industrial Control Systems (SICS) Framework builds on the previous guidance which has been used by organisations worldwide. While not a standard, the framework incorporates the latest industry good practice and experience from the fields of ICS and IT security to address ICS security.

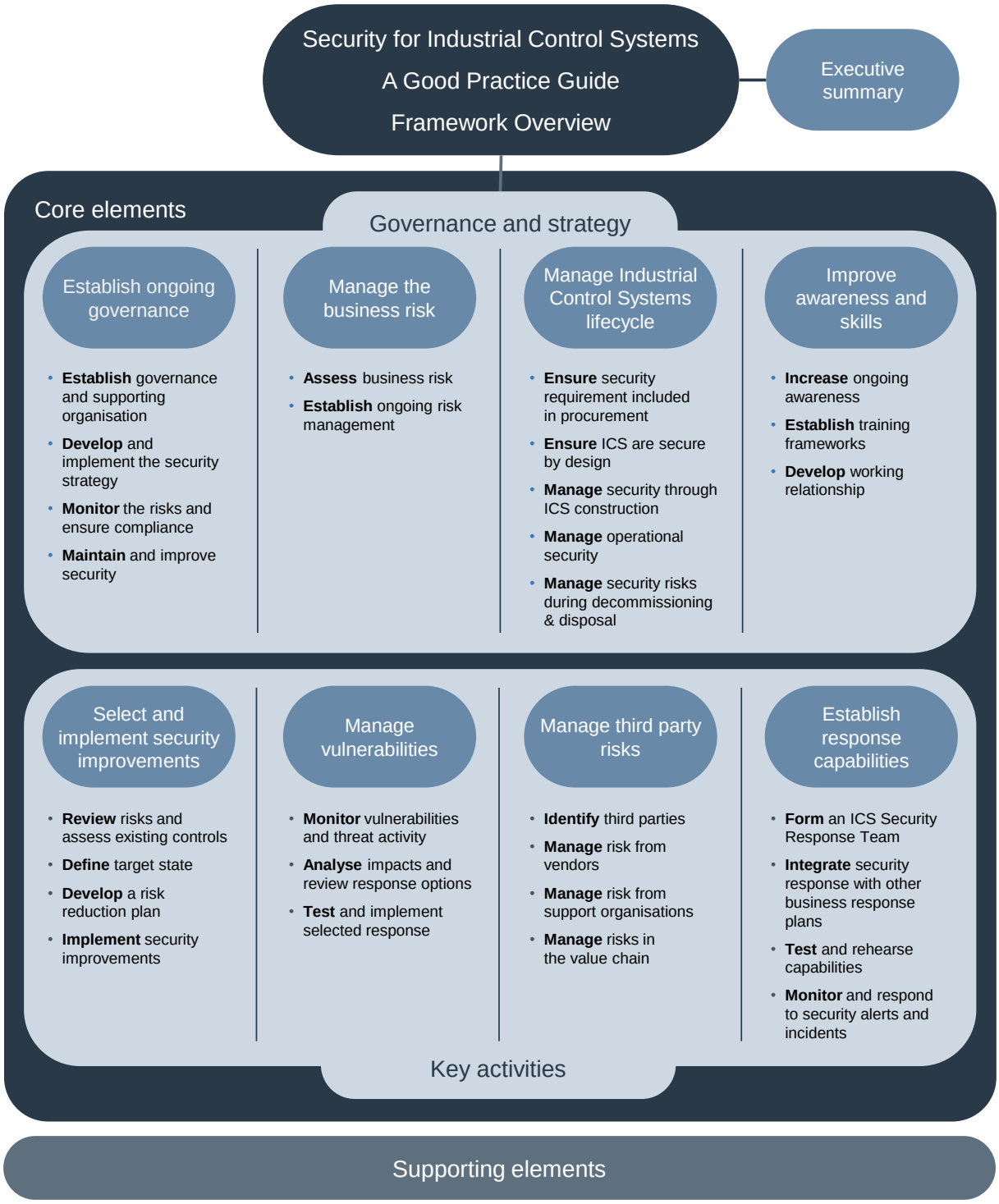
The framework consists of:

- An Executive Summary
- A Framework Overview containing the objectives, good practice principles and guidance required for an ICS security programme
- Eight core elements covering the governance and strategy, and the key activities to achieve the ICS security programme.

[1] https://ics-cert.us-cert.gov/advisories/ICSA-10-272-01

[2] https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01

[3] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B


Security for Industrial Control Systems
A Good Practice Guide
Framework Overview
Executive summary
Core elements
Governance and strategy
Establish ongoing governance
Establish governance and supporting organisation
Develop and implement the security strategy
Monitor the risks and ensure compliance
Maintain and improve security
Manage the business risk
Assess business risk
Establish ongoing risk management
Manage Industrial Control Systems lifecycle
Ensure security requirement included in procurement
Ensure ICS are secure by design
Manage security through ICS construction
Manage operational security
Manage security risks during decommissioning & disposal
Improve awareness and skills
Increase ongoing awareness
Establish training frameworks
Develop working relationship
Select and implement security improvements
Review risks and assess existing controls
Define target state
Develop a risk reduction plan
Implement security improvements
Manage vulnerabilities
Monitor vulnerabilities and threat activity
Analyse impacts and review response options
Test and implement selected response
Manage third party risks
Identify third parties
Manage risk from vendors
Manage risk from support organisations
Manage risks in the value chain
Establish response capabilities
Form an ICS Security Response Team
Integrate security response with other business response plans
Test and rehearse capabilities
Monitor and respond to security alerts and incidents
Key activities
Supporting elements

How do I use it?

The framework and its supporting elements are intended to be a point of reference for an organisation to begin to develop and tailor ICS security that is appropriate to its needs.

This framework can be used in a number of ways:

1. The Framework Overview can be used by all to understand the entirety of the framework and the reasoning behind each of the core elements. It can also be used as a tool to communicate the importance of ICS security and how it can be achieved.
2. The entire SICS Framework can be used to structure a complete ICS security programme or individual elements can be used to tailor an existing programme.
3. Those requiring more detail on how to implement certain core elements as part of an existing ICS security programme can reference the individual guides.

The benefits

Through using the SICS Framework, an organisation can reap the benefits of having more secure and resilient systems operationally, and in their enhanced ability to deal with a cyber attack. Better security can also enable businesses to prosper by allowing them to exploit new technologies securely. Without appropriate security, organisations face being left behind or exposing themselves to unnecessary and sometimes avoidable risk. Only by understanding and mitigating these risks can an organisation take full advantage of advances in technology and new ways of working. While security cannot prevent all risks materialising, it can help to reduce the likelihood and potential impact allowing organisations to recover faster and return to business as usual.

Through implementing the SICS Framework, businesses can ensure that the right technologies and processes are in place. This can support a suitably informed and trained workforce and maintain the security of ICS throughout the life of the system and of future systems. Finally it can help to ensure that the evolving risks associated with ICS are monitored and managed through supporting organisations in a consistent and appropriate manner.

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/