CESG

CPNI
Centre for the Protection
of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

MANAGE THIRD PARTY RISKS

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:	

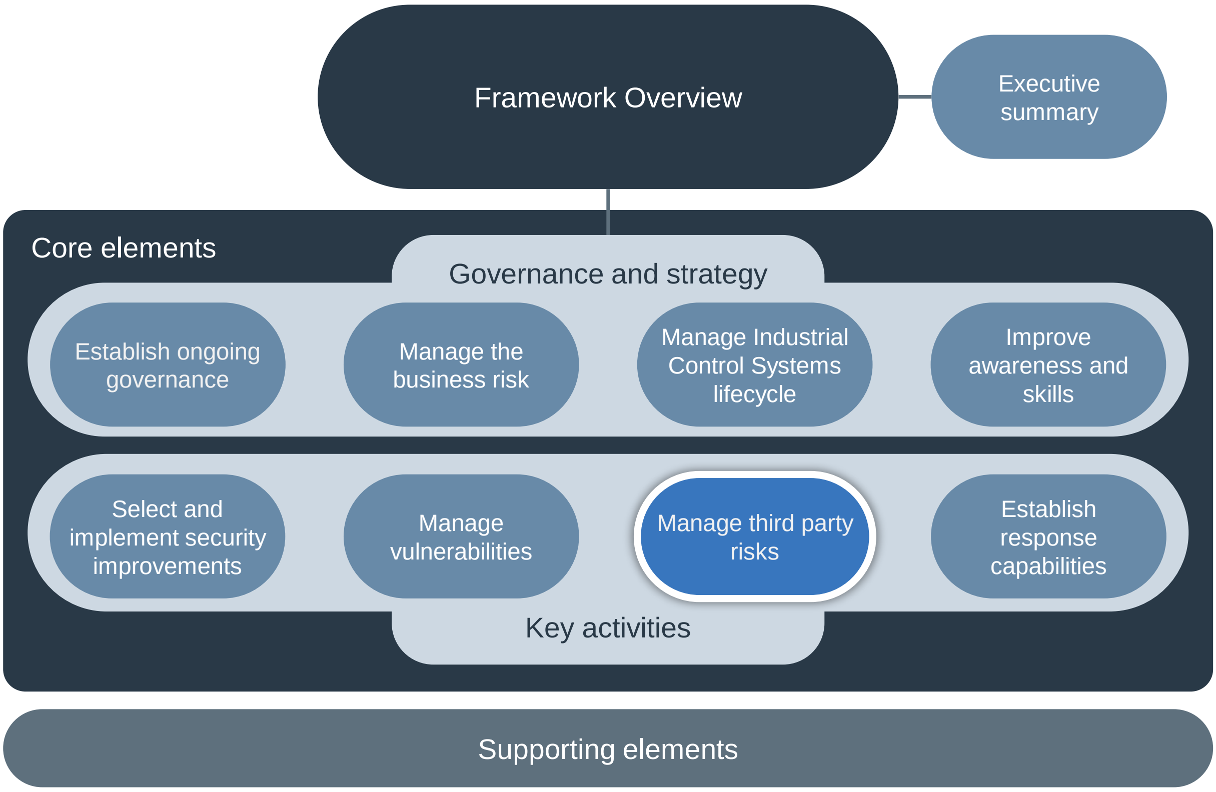
CONTENTS

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 Manage third party risks - summary

The objective of this guide is:

- To identify key third parties and effectively manage the associated risks that may have an impact on the security of an organisation's ICS.

The security of an organisation’s ICS can be put at significant risk by third parties, e.g. vendors, support organisations and other entities in the value chain and therefore warrants considerable attention. Technologies that allow greater interconnectivity, such as remote access or internet connectivity, bring new threats from outside the organisation. Third parties are often considered a weak link and must therefore be engaged as part of the ICS security programme at the earliest stage and steps should be taken to reduce the associated risk.

In the past ICS were often bespoke systems that were developed in house but nowadays most ICS are configured by third party integrators and vendors. Consequently third party products and services are present in almost all ICS, bringing with them a number of associated risks.

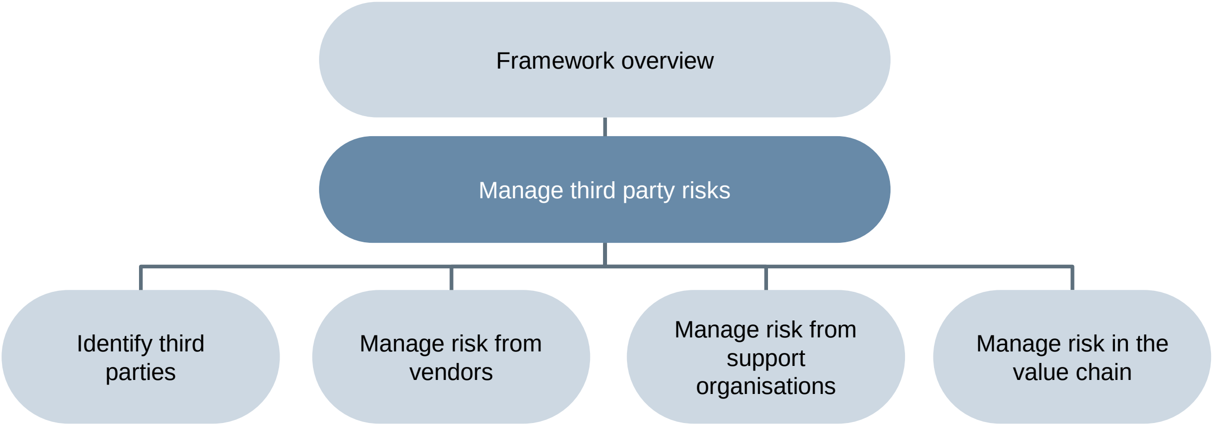
Awareness or visibility of the third party risks is the key to enabling an organisation to begin to manage them. The recognition of potential security gaps enables the organisation to seek appropriate engagement with vendors and support organisations in order to mitigate the identified risk.

The common perception of third party risk relating to ICS is that it is focused on remote access connections to the operational ICS. However, the picture is much wider than just this technical concern and should also be considered and managed in terms of the ICS lifecycle, see SICS Framework element 'Manage the ICS Lifecycle'. There are different categories of third parties such as ICS vendors, support providers and different elements in the value chain. Each of these has their own related issues.

When considering the vulnerability of ICS, the importance of assessing the wider value chain can easily be overlooked. Seemingly innocuous systems that provide systems support can have significant direct or indirect impact on critical systems.

To manage the risk from third parties there are four good practice principles that should be followed, these are shown in Figure 2.

Figure 2 – Good practice principles to manage third party risks



2 IDENTIFY THIRD PARTIES

The identification of third parties associated with ICS assets enables the organisation to plan and mitigate the risk that they pose.

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

- Identify and engage early with all third parties, including vendors and service providers, and all other links in the value chain that are associated with the ICS.

2.1 Create a list of ICS third parties

A list of third parties can be derived from many sources including procurement contracts (see SICS Framework element 'Manage Industrial Control Systems lifecycle') and ICS teams. An ICS inventory can also provide a good starting point for identifying all third parties. The production of an ICS security inventory is described in greater detail in SICS Framework element 'Manage the Business Risk' however it should, at the very least, contain information on:

- What the system is
- The owner
- Current versions of hardware and software.

For each item in the inventory, organisations should determine what third parties are associated with each item. It may be that an inventory item is associated with a number of different third parties as defined in the table below. When performing this analysis the following questions should be asked:

- **Value chain:** who is part of it and what processes / activities are they involved in?
- **Vendors / suppliers:** who is the system vendor, who is the sub-system vendor and which sub-contractors are involved?
- **Service providers:** who provides it and how and what service level agreements exist?

Definitions

Vendor: A person, organisation or integrator that provides software, hardware, firmware and/or documentation to the organisation for a fee or in exchange for services.

Support: The 'provision of capabilities for' or the ability 'to interface to' the ICS. e.g. monitoring systems, resetting passwords, problems, bug fixes, etc.

Sub-contractor: Person or entity that enters into a contractual agreement with a prime contractor to perform a service or task.

Value chain: Organisations involved in the process of activities inherent to the operation of a company. E.g. for an oil pipeline the value chain could include an oil refinery operated by another organisation.

The time needed to collate the initial list of third parties and review is dependent on the size of the ICS inventory. Care should be taken to strike an appropriate balance when capturing third party data. Further analysis during later stages may not be possible if too little information is recorded but it may be difficult to maintain a list if it contains too much information. Where third party information was not available in sufficient detail during the inventory collation, this information should be sought as part of this element of the framework. Any new information should be added to the inventory and kept up to date.

Another important factor to consider when creating a third party inventory that can help in striking this balance is how items are categorised and prioritised in terms of risk. For instance a company that performs remote maintenance of a key system will most likely present a higher risk than a payroll supplier. Prioritisation can help in the targeting of limited resources to ensure that the greatest risks to the organisation are addressed first.

3 MANAGE RISK FROM VENDORS

Organisations can develop in-depth knowledge of product security functions and can influence the security functionality of both existing and new products by developing relationships with ICS vendors.

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

- Ensure that security clauses are detailed in all procurement contracts prior to agreements and are cascaded down to sub-contractors.
- Engage with all vendors on an ongoing basis to ensure:
  - Current and future discoveries of vulnerabilities within the systems that they supply are identified and notified promptly to the user organisation
  - The organisation understands the security architecture of the ICS provided by vendors and how they may be supported remotely
  - Vendors understand the organisation's architecture in order to provide secure ICS.
- Request vendors to provide security guidance (including system hardening) for their current ICS and a roadmap for future system development utilising a secure development lifecycle (SDLC).
- Ensure that all vendors incorporate appropriate anti-malware protection within their ICS.
- Establish an effective software patching process with the vendor.
- Agree with the vendor system hardening procedures for the ICS in operation.
- Identify all component technologies (e.g. databases, open source software) used within the ICS to ensure that all vulnerabilities are managed.
- Undertake regular security reviews and audits of all vendors according to risk based priorities.

3.1 Understand vendors

By engaging in productive dialogue with the ICS vendors, the organisation can build a relationship that allows it to understand the capabilities and limitations of the vendor’s products and services. This relationship will also enable the organisation to better communicate their specific application needs, the types of security risks they are exposed to, and the associated security requirements to the vendor. This may include enhanced security features and greater compatibility with other security solutions.

There are a number of key security aspects that will benefit from a two-way dialogue with vendors which are described in the following sections.

3.2 Contractual measures to manage vendor risk

Creating the correct contractual framework is an essential part of managing vendor risk and should be considered as part of the ICS lifecycle during the procurement stage, see SICS framework element 'Manage Industrial Control Systems lifecycle'. Much of this is likely to have been done by either the organisation's legal or procurement departments but it is important that specific ICS security clauses are included within any contracts with vendors. This ensures that risks are managed as part of the contract where typical security clauses include:

Non-disclosure agreement: the vendor may be exposed to sensitive information (e.g. system design information, IP addresses) about the organisation and it is essential that this is not exploited or used without the permission of the organisation. This can range from an understanding of the firewall rule set, to specific system information. In particular the vendor should not publish information about the organisation without explicit permission and only after a review of the security implications.

Vulnerability disclosure: it is important that current and future vulnerability discoveries are communicated by the vendor to the system owner so that they can be managed and actioned appropriately. Further guidance can be found in SICS Framework element 'Manage vulnerabilities'.

Background checks / internal security checks: the organisation should request assurance from vendors that staff and contractors have had the relevant background security checks prior to taking up employment and are maintained on an ongoing basis. Further details on pre-employment screening can be found in the CPNI guide, A Good Practice Guide on Pre-Employment Screening[1], on the CPNI's Personnel Security Measures website[2] and within BS7858 'Security Screening of Individuals Employed in a Security Environment[3].

Approved vendor list: building ICS security requirements into preferred vendor selection and certification is an extremely powerful process to ensure that the desired security culture and approach is embedded in procurement decisions. Organisations will need to develop their own selection criteria where existing security schemes such as Cyber Essentials[4] can provide a good starting point. The resulting approved vendor list can save the organisation time and money by reducing duplication and providing assurance about potential vendors. From the vendor's perspective, there is an incentive to get on the approved vendor list as this can be a good source of future business.

Secure development and testing: the organisation should ensure that vendors follow a secure development and testing process that is commensurate to the criticality of the ICS that is being procured and operated. Testing should not be limited to products but also include PLC and controller code.

Security requirements throughout the ICS lifecycle: where projects for new processes or new systems are planned it is essential that security is included early on in contractual discussions, particularly if new vendors are involved. Additionally security must be maintained and reviewed throughout the whole lifecycle (design, build, operation, and decommissioning), see SICS Framework element 'Manage Industrial Control Systems lifecycle'.

Security reviews and audits: regular security performance reviews should be undertaken with the vendor to discuss outstanding security issues, progress against mitigation and improvement plans and to discuss the security road map. The audit process to assess third parties should be defined by the organisation.

Secure technology sourcing: organisations should require vendors to use reputable and assured technology sources for the products and services they are providing. Vendors are likely to have an

[1] http://www.cpni.gov.uk/documents/publications/2009/2009024-gpg_pre_employment_screening.pdf

[2] http://www.cpni.gov.uk/advice/Personnel-security1/

[3] http://shop.bsigroup.com/ProductDetail/?pid=000000000030237324

[4] https://www.cyberstreetwise.com/cyberessentials/

extensive supply chain which can introduce additional risk, for example a laptop unknowingly preinstalled with malware. This is particularly important where the product or service is part of a critical system where the impact could be severe.

The Cyber Security Procurement Language for Control Systems document by US DHS[5] provides further details on this subject.

3.3 Key vendor related security measures to consider

There are a range of ways to mitigate vendor related risk, examples include:

Anti-malware: work with vendors to ensure that anti-malware protection is incorporated into their ICS.

Logging and monitoring: work with vendors to ensure that appropriate system information is logged and systems can be actively monitored by the organisation or a third party. This can be particularly useful in alerting an organisation to a potential security incident through the monitoring of system and network performance.

Patching process: agree with vendors what process they will use for testing and accrediting security patches for both the underlying operating system and the ICS software. Questions for consideration are:

- Do they accredit patches?
- Will they notify customers and deploy accredited patches?
- How long does it take to accredit?
- Are there installation notes or guidance on the patches that should be deployed?

Some vendors are keen to test all security patches prior to approval for deployment. This may involve a stipulation that only patches and updates received directly from the vendor are valid for updating the system. This approach can lead to delay, so it is important to work closely with the vendor to ensure that the security needs of the organisation are met, and that the vendor is aware of any additional delays that they might cause. All security patches should be accredited and approved through a change control process prior to any deployment.

System hardening guidance: many systems and devices will support unused and unnecessary functions and network services. Given that an organisation will have relatively specific requirements, it is important that the remaining unused functionality is disabled to eliminate unnecessary security risk. Additionally most ICS devices are initially provided with security functions disabled allowing them to perform their full range of functionality. Vendors should be engaged to provide guidance on locking down and hardening their systems and selecting appropriate secure functions of the device.

Component technologies: most ICS applications have component technologies that pose a potential security risk if not maintained and patched when necessary. Examples include the use of third party and open source technologies or database components in ICS where the functionality is not apparent to the user.

Remote support: a significant risk area that needs to be addressed through engagement with vendors is remote support. Such support should be provided through a secure connection. The systems from which the vendors connect should also be secure, both physically and electronically. The personnel that connect in should have completed background checks and be appropriately trained and any client confidential information (such as system documentation) should be properly secured. Organisations should seek assurance (possibly through site visits or audits) on these topics. See Section 4 of this element for further details.

Security Testing: organisations should require vendors to undertake security testing of their products to identify and eliminate security vulnerabilities. This should include system design reviews, lab testing

[5] https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

and penetration testing. Recent research had highlighted a number of security vulnerabilities in low level control devices such as remote terminal units (RTUs) and programmable logic controllers (PLCs). Organisations should seek assurance from suppliers and vendors that these low level control devices have been appropriately analysed to identify what ports and services are being used and whether there are any known vulnerabilities. Organisations should require the vendors to carry out testing on ICS and their components (such as PLCs) to ensure they are free from security vulnerabilities. Further guidance on testing and assurance of embedded control devices is set out in SICS Framework element 'Manage Industrial Control Systems lifecycle'.

Disclosures of system communications: organisations should encourage vendors to detail which ports are used, along with the protocols used.

SICS Framework element 'Select and implement security improvements' details other security measures that can be implemented to manage vendor related risk.

3.4 Embedding the security culture in vendors

The organisation should be looking to influence the vendor's security culture so that it meets or exceeds their requirements. Typical activities that create a solid security culture and should be encouraged / mandated with vendors include:

- Regular security reviews
- Security audits
- A culture of security and awareness
- Open dialogue about vulnerabilities, alerts and incidents
- Security roadmap for vendor improvements
- Relationships with security vendors
- Certification schemes for vendors and products e.g. ISASecure[6].

3.5 Influencing the vendor security roadmap

A key benefit of building a good working relationship with vendors is the opportunity it creates to work with them to influence the direction and pace of their security development i.e. the vendor's security roadmap. This is a potential 'win-win' as the vendor can get valuable market insights and the organisation can mitigate vulnerabilities through the improvement in the vendor's products and services. This can be accomplished with one-to-one or one-to-many relationships through membership in established vendor security forums. Where these forums do not exist, organisations should encourage their creation.

Advances in the certification of anti-malware software and operating system patches by a number of key vendors has been influenced to some extent by the purchasing power of a number of large organisations looking to improve the security of ICS. By engaging in an ongoing dialogue with the vendors, organisations were able to communicate their priorities and concerns at the inability to protect against malware. The communication of these requirements from a number of organisations enabled the vendors to build business cases to allow for research and development in this area. This resulted in better security features in their ICS products.

[6] http://www.isasecure.org/en-US/Certification

4 MANAGE RISK FROM SUPPORT ORGANISATIONS

By developing a relationship with third party support organisations the related potential security risk can be managed.

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

- Undertake regular risk assessments of support organisations and ensure any required countermeasures are implemented.
- Prevent access to the ICS by support organisations until appropriate measures to prevent or reduce potential security breaches have been implemented. Issue and agree a contract defining the terms of the connection.
- Engage with all support organisations on an ongoing basis to ensure all security incidents that may have a security impact on the organisation are reported.
- Increase awareness in all support organisations so they fully understand the ICS that they are supporting and agree to work in accordance with agreed security procedures.

4.1 Understand support organisations

In common with other areas within the IT environment, there are many ICS that are supported in some way by third parties. Consequently the security of ICS is often critically dependent on the support organisation and the services that they provide, such as:

- Network and telecommunications provision and support
- IT infrastructure management
- Hardware support for spares and repairs
- Application and system monitoring and support.

Using third party support gives an organisation access to specialist resources whilst reducing the cost associated with training and recruitment. However, this has also increased the level of risk to organisations by creating a dependency on the security of others. Therefore when new technologies or services are introduced, it is the third party who must ensure that they have the appropriate resources to provide effective support. Any failing could have an undesirable impact on an organisation's ICS.

In addition to the common services described above, organisations may have used third parties to provide additional security and administration services as part of the wider security architecture. Examples of such services include:

- System operation, security and performance monitoring

- Security patching
- Firewall management and monitoring
- Intrusion detection monitoring
- Anti-malware protection
- Threat intelligence
- Regular security monitoring routines e.g. log monitoring, remote access connections, password changes etc.

Choosing which services could be supported by a third party needs to be based on the criticality of the system, the support required, availability of appropriately skilled resources whether internal or external, and maintenance scope.

Organisations need to assess the risks that can be introduced from the use of third party support organisations including:

- Remote support connections
- Personnel security
- Contractual issues
- Security awareness and training
- Physical security
- Confidentiality.

Third party support organisations often perform similar functions and services to ICS vendors. Consequently the good practice principles are very similar to those drawn up for managing vendor risk and focus on the need to have clear contractual agreements, good working relationships, and clear communication channels.

Further details on outsourcing can be found in CPNI - Outsourcing: Security Governance Framework for IT Managed Service Provision[7].

4.2 Remote support connections

Third party support must ensure that any new technology introduced to a secure ICS is authorised by the organisation. The addition of devices such as modems or routers to enable remote or out-of-hours support are a potential risk and must only be used with the prior authorisation of the organisation and should be appropriately secured. There is likely to be a trade-off between convenience and security and many third parties may offer significant price reductions by offering remote support. To minimise the risk associated with this approach the following actions should be considered:

- Denial of access until connections are protected
- Ensure systems from which support organisations connect are secure both physically and electronically
- Ensure that access rights are regularly reviewed and audited
- Monitor the actions of the users connecting via these connections
- Ensure that facilities and systems from which the support organisation connects are secure, both physically and electronically
- Ensure that all client confidential information (such as system documentation) is stored securely
- Ensure the connection is controlled by the organisation and is only enabled for pre-agreed purposes
- Connections have a time limit applied.

[7] http://www.cpni.gov.uk/Documents/Publications/2006/2006027-GPG_Outsourcing_IT.pdf

Organisations may wish to obtain assurance on the above topics via site visits, reviews or audits.

Please refer to the CPNI and US DHS - Configuring and managing remote access for ICS[8].

4.3 Personnel security

A key part in any system security framework is the human element. Personnel security aspects should be considered when assuring the security of third parties. All personnel should complete appropriate background security checks as a routine part of the third parties' recruitment process.

Further details can be found on pre-employment screening (CPNI - A Good Practice Guide on Pre-Employment Screening[9] and within BS7858[10]) and continual screening (CPNI - Ongoing Personnel Security[11]).

4.4 Vendor contractual issues

There are a number of security elements that should be considered in any third party support contract:

- **Right to audit:** clauses to ensure the right to audit or review third party services and procedures, systems and premises.
- **Confidentiality of information:** clauses to ensure the confidentiality of an organisation's confidential information (such as system documentation). This is dependent on the organisation correctly classifying information. Ensure a non-disclosure agreement is in place.
- **Cyber security requirements:** clauses to ensure that the third party organisation is committed to maintaining an appropriate level of cyber security
- **Appropriate service level agreements:** ensure that the service levels are clearly defined in the contract and that they are appropriate to the organisation's requirements.

4.5 Security awareness and training

Third party support personnel should have an appropriate level of security awareness. Not everyone needs to be a security expert but individuals should have the appropriate technical, procedural and operational security awareness so they can perform their role securely. This may include:

- **Policy and standards:** ensure that all personnel are aware of what policies and standards are in place for the systems being supported.
- **Specific business security processes:** the organisation may have specific security processes that will need to be communicated to third parties.
- **Response and continuity planning:** ensure that a third party support organisation has appropriate response and continuity plans in place.
- **Skills:** there are a number of industry standard qualifications associated with security and support, but it is important to gain assurances that the personnel have both the appropriate practical knowledge and formal qualifications.

Further information can be found in SICS Framework element 'Improve awareness and skills'.

[8] http://www.cpni.gov.uk/documents/publications/2011/2011006-remote_access_for_ics-viewpoint.pdf?epslanguage=en-gb

[9] http://www.cpni.gov.uk/documents/publications/2009/2009024-gpg_pre_employment_screening.pdf

[10] http://shop.bsigroup.com/ProductDetail/?pid=000000000030237324

[11] http://www.cpni.gov.uk/documents/publications/2014/2014006-ongoing-personal-security.pdf?epslanguage=en-gb

5 MANAGE RISK IN THE VALUE CHAIN

Linking ICS to other elements in the value chain can provide significant business benefits in terms of lower costs and increased efficiencies. However such connections can introduce security risk through the implementation of network or system connections to external systems. Tighter integration into the value chain can introduce harder dependencies and make the whole chain less resilient to disruptions to individual systems. Consequently a security event in one system could impact the whole chain and cause disruption to many other systems; possibly across a number of different organisations. Where systems form part of a larger value chain it is important to assess the upstream and downstream dependencies and ensure they are all appropriately protected with security measures and response capabilities.

Value chain: organisations involved in the process of activities inherent to the operation of a company

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

- Ensure connections to any organisation in the value chain are secured on both sides and that the third party organisation provides assurance that their security risks are managed. Examples of such organisations include: suppliers, distributors, manufacturers, customers or joint ventures.

5.1 Understand the value chain

Understanding the value chain itself and the dependencies that exist within it is critical to managing risk. The organisation should also identify the critical paths within the value chain. Where systems or connections span organisational boundaries, clear arrangements for security responsibilities should be agreed by the relevant parties.

There is a danger that many of the specific functions or processes within a value chain operate in a 'silo' mentality and are only concerned with what they need to do. Instead each part of the value chain needs to consider the wider strategic risk and understand the part they play in its security.

Value chain connections will vary significantly from one industry to another and can include those that are linked to operational or business functions. Examples of some third party value chain connections are:

- Operational
  - Utility providers (e.g. gas, water, electricity, compressed air, steam etc.)

  - Power generation, distribution and transmission
  - Oil and gas production systems
  - Pipelines (upstream and downstream).
- Business
  - Energy trading systems
  - Tanker loading facilities
  - Joint venture partners for production reporting
  - Automated stock ordering systems.

There are two key risk areas that should be considered for each value chain interface:

1. Interface security
2. Value chain dependencies.

5.2 Interface security

System interfaces between ICS can be a potential backdoor into the ICS and could provide a route for infection from malware or unauthorised access. Such connections might take a variety of forms including:

- Serial lines
- Modem connections
- VPNs
- Connections via other networks
- Removable media e.g. USBs
- The internet.

All such connections should be clearly identified, included in the ICS inventory, documented in system and network diagrams, and should be appropriately secured and monitored. Disconnection plans should be established as part of response and continuity plans.

In addition to considering these connections for interface security their potential value chain dependencies should be assessed, as described below.

5.3 Value chain dependencies

Each element in the value chain should be assessed in terms of ICS security threats. Where there are critical dependencies, i.e. where the organisation's systems are dependent upon other systems (either upstream or downstream), then assurance should be sought from the relevant third parties. This should cover how those systems are protected from an ICS security point of view. In order to gain this assurance, organisations may consider security reviews, health checks or audits. If deemed necessary based on prioritisation, appropriate response and continuity plans should be put in place for each value chain dependency.

6 CASE STUDY: ON-TRACK RAIL

6.1 On-Track Rail

On-Track Rail is a regional railway company that runs the public railway system in a particular region and is one of a number of organisations that make up the national railway system.

The company recently went through a major renewal of their ICS involving the replacement of legacy systems with state of the art systems using standard IT technologies. The upgraded system was interlinked to the surrounding regions allowing for the uninterrupted movement of trains between regions.

6.2 Identify third parties

As part of the Critical National infrastructure (CNI) On-Track Rail needed to identify the third parties that would be supplying their systems and who would be configuring and maintaining them. Additionally the organisation wanted to identify the systems that were connected to the new ICS.

Following this review the organisation identified the following third parties:

- ICS Vendor1, with the following sub-contractor
  - Hardware Supplier 1
  - Hardware Supplier 2
- ICS Vendor2 with the following sub-contractor
  - Component Manufacturer
- ICS Vendor 3
- ICS Integrator
- Region A ICS
- Region B ICS
- Support Group1 for networking
- Support Group 2 for server support.

6.3 Managing the third party risk

Ahead of the renewal, On-Track Rail engaged with the three ICS vendors to understand the security measures that each of them offered and how this would fit their security requirements. Following this initial work On-Track Rail decided to use an independent organisation to carry out security testing of each of the vendors’ proposed solutions.

Security testing discovered vulnerabilities in each of the vendors' proposed solution. All three were contacted regarding these vulnerabilities however only two responded with a patch to fix them.

Patches were applied and solutions re-tested to validate that the vulnerabilities had indeed been fixed. As a consequence On-Track Rail decided that ICS Vendor 3 would not be considered as a supplier for their upgraded ICS and was removed from their approved vendor list.

6.4 Support organisations

The new ICS was configured to allow support organisations to remotely connect to carry out activities such as troubleshooting and installing security patches.

The contracts for the support organisations were updated from the standard contract to include security requirements for each vendor prior to being agreed with the support organisations. These requirements included:

- All remote connections must be controlled by On-Track Rail and granted for only a time period sufficient to carry out the activity
- Only named individuals are allowed carry out specific activities
- All named individuals must be appropriately security checked on an ongoing basis.

Having also recognised that this was a new area for both support organisations, On-Track Rail developed a series of ICS security training courses aimed at the personnel carrying out the ICS support. Following this successful training by On-Track Rail, the support organisations agreed to deliver the training more widely within their own organisations to improve the awareness and skills of their personnel.

6.5 Managing risk from the other regional organisations

Having identified that the ICS required interconnectivity with the other regional rail organisations and that this risk posed a threat across the rail network value chain, a number of the organisations, including On-Track Rail, developed a working group to identify how the risk could be minimised.

This working group was eventually expanded to all regions. An agreement was reached that interfaces between the ICS of different organisations required an industrial firewall. The firewalls used would have to be independently certified to an agreed standard.

The group recognised that improved information sharing was vital should one region have an ICS security incident therefore it was also agreed that incident information should be shared amongst the regional organisations.

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/