CESG

CPNI
Centre for the Protection
of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

MANAGE VULNERABILITIES

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:

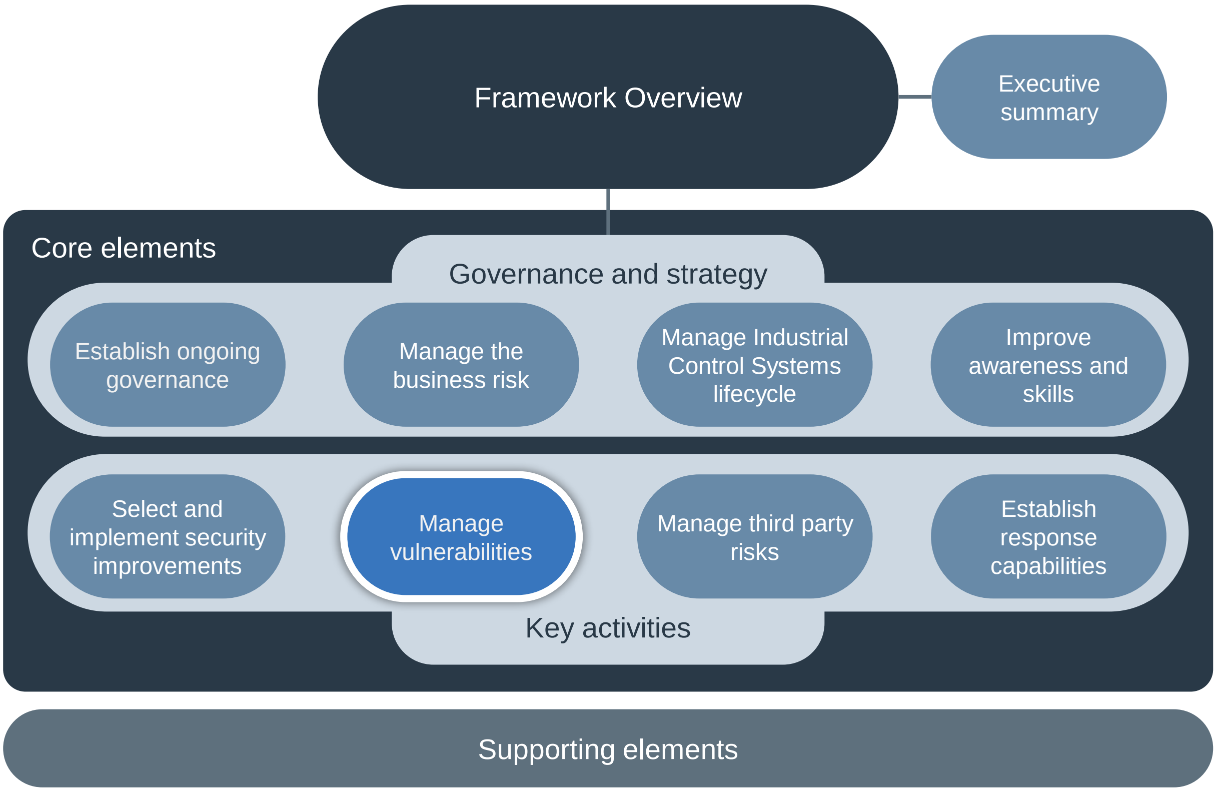
CONTENTS

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 vulnerabilities - summary

The objective of this guide is:

- To establish the procedures necessary to monitor, evaluate and take appropriate action in response to newly published vulnerabilities and changes to the threat landscape.

Implementing and maintaining security in ICS environments is fundamental to ensuring that risks are managed on an ongoing basis. Two main drivers that impact the changing risk profile are changes in vulnerabilities and changes to threat activity.

In the past few years prior to the writing of this new framework element, there has been a significant increase in the capability and motivation of those threatening ICS, resulting in a rising risk profile. The first major visible sign of this was the Stuxnet malware. Analysis of the malware by the security community revealed it to be a very cleverly crafted attack, utilising a number of zero day vulnerabilities, and with a payload targeting a very specific ICS configuration. Equally significant in 2014, two wide-ranging vulnerabilities were published within months of each other that affected Open SSL[1] libraries and the popular Unix shell, bash[2].

These are far from being isolated events and, in the past few years, attacks and vulnerabilities affecting ICS have multiplied including:

- **2010 – Stuxnet malware** attacked the Iranian nuclear fuel processing industry
- **2011 – Night Dragon malware** stole valuable information from oil and gas companies
- **2012 – Shamoon attack** caused massive business disruption after around 30,000 computers were taken out of service in Saudi Aramco
- **2014 – Havex attack** saw energy and utilities companies being targeted through spam e-mails and compromised vendor websites
- **2014 – BlackEnergy** malware targets specific ICS products from specific vendors used in critical infrastructures.

Another issue to be considered is that normal information assurance approaches used in the enterprise environment may not be suitable for ICS. Such systems often face different challenges and constraints and although these can be subtle differences, it is important to address them, particularly when developing information security requirements and preparing incident response plans.

An example is the risk that arises during the time when ICS vendors are testing and accrediting security patches or software updates prior to their deployment on live systems. As a result, systems may be vulnerable to attack, and suitable countermeasures should be considered.

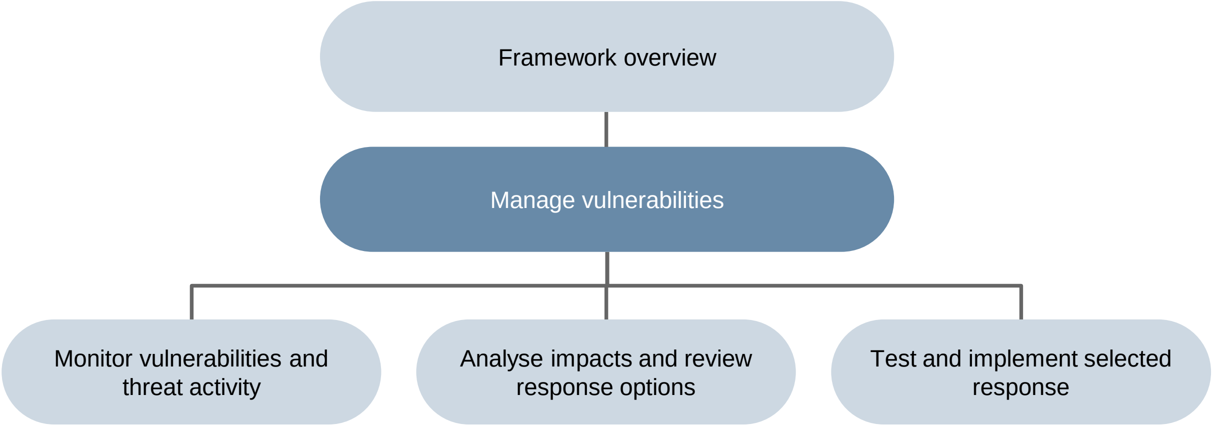
Throughout the SICS Framework, the guiding principles are protect, detect and respond. This document contains guidance on the actions necessary to respond to these principles and are summarised below and set out in Figure 2.

- Monitor vulnerabilities and threat activity
- Analyse impacts and review response options
- Test and implement selected response.

[1] https://www.cert.gov.uk/resources/advisories/heartbleed-bug/

[2] https://www.cert.gov.uk/resources/advisories/update-bash-vulnerability-aka-shellshock/

Figure 2 – Good practice principles to manage vulnerabilities


Framework overview
Manage vulnerabilities
Monitor vulnerabilities and threat activity
Analyse impacts and review response options
Test and implement selected response

2 MONITOR VULNERABILITIES AND THREAT ACTIVITY

Maintaining awareness of new vulnerabilities and constant changes to the threat landscape can be difficult. Access to the right information sources and good knowledge of the ICS environment is necessary to identify the relevant information from the large quantity of daily alerts and advisories. To do this effectively requires a dedicated process and identified resources.

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

- Implement a vulnerability management process to ensure that vulnerabilities are kept to a minimum in the ICS environment.
- Ensure that new published vulnerabilities affecting the technologies used in the ICS are known about through continuous monitoring of subscriptions to specialised information sources (including CERTs, ICS vendors, and those providing underlying software used in the ICS – e.g. Microsoft).
- Regularly assess the current threats to ICS. Such an assessment should include: monitoring the reports of similar ICS infrastructure in related sectors being targeted, drawing on open source intelligence or participating in special interest groups to determine whether the risk profile is changing.

2.1 Preparing the organisation for effective vulnerability management

Vulnerability management is more than just patching systems and encompasses the following key processes:

- Monitor new vulnerabilities and threats
- Conduct vulnerability assessments on the infrastructure
- Respond to vulnerabilities including target timelines for remediating critical vulnerabilities
  - Authorise changes to respond to vulnerabilities
  - Test and deploy responses (e.g. patches and modifications).

These activities require specialist skills and may be time intensive and critical. It is vital that the team or individuals responsible for vulnerability management are appropriately trained and resourced in order to operate in line with the needs of the business (i.e. extended opening hours, 24/7). Organisations may resource this internally with individuals working as part of a virtual team or on a part time basis. In certain circumstances an organisation may choose to allocate these activities along with other security responsibilities (e.g. security monitoring, security management) to a dedicated team (e.g. to a Security Operation Centre).

There are several things that an organisation can in preparation for effective vulnerability management by simplifying the process and ensuring that the right information is available. These include:

- Maintain an asset and configuration database
- Operate a standardised ICS architecture
- Establish relationships with vendors and third parties.

2.1.1 Maintain an asset and configuration database

To best target the effort associated with patch management, it is important that the organisation maintains an asset register that contains sufficient information for effective vulnerability monitoring, analysis, and response.

In this context, it is essential that in addition to details of hardware, the asset and configuration database contains information on firmware and software configuration, including the vendors and version for all ICS in operation and in development.

2.1.2 Operate a standardised ICS architecture

In order to minimise the effort required to manage vulnerabilities, it is recommended that the technologies used in ICS configurations are standardised as far as possible across the organisation. This will limit the quantity of different products to be managed. Maintaining a consistent ICS estate also provides an advantage in reducing the need for different reference test platforms where vulnerabilities can be assessed, solutions tested and validated before deployment.

However, there is a balance to be struck as full standardisation could result in vulnerabilities having the potential to affect a larger part of the estate and lead to increased exposure. An effective mix of technologies will prevent vulnerabilities spreading and create a defence-in-depth architecture. For example, it is common practice to use different firewall technologies to avoid them being exposed to the same vulnerabilities. This principle may be extended to other technologies (e.g. different anti-malware on workstations and servers, or different technologies for perimeter components and for core systems). Further information on improving defences can be found in the CPNI iDATA programme[3].

2.1.3 Establish relationships with vendors

When selecting products, one of the key criteria used should be how updates are managed by the vendors this includes considering:

- How vulnerabilities are disclosed, managed and security patches made available for the product
- How secure is the mechanism for ensuring integrity and authenticity of new patches and releases
- How third party software updates are supported (OS updates, anti-malware upgrades, databases patches). Often those changes are subject to accreditation by the vendors. This is a specific constraint to take into account when applying patches and more general changes to ICS.

More information on vendor selection and engagement is available in SICS Framework elements ‘Manage ICS lifecycle’ and ‘Manage third party risks’.

2.2 Monitor the right information sources for vulnerabilities and threats

There are a lot of information sources covering newly discovered vulnerabilities and threats. Monitoring all of them is not possible so it is necessary to carefully select information sources so that they cover the most critical technologies that are in operation and notify new discoveries quickly.

[3] https://www.cpni.gov.uk/advice/cyber/idata/

Another criterion in selecting information sources is how notifications are sent. Some provide information in a repository and the user has to sort through all data to retrieve the alerts and notifications which are applicable to them. Others, usually in a commercial service from vendors or specialist security organisations, provide tailored alerts for users that only relate to the specific technologies which they operate.

Whatever option is used, organisations need to consider the level of coverage of the information source, the level of analysis provided and the speed they publish information. This is vital in order to minimise the window of exposure (further details on the window of exposure can be found in the ENISA document 'Window of Exposure a real problem for SCADA systems'[4]).

The main sources of information in this area are:

- Computer Emergency Response Teams (CERTs):
  - CERT UK[5] - providing national advice for critical infrastructure operators in the UK
  - ICS CERT[6] - from US Department of Homeland Security which provides focused advice on ICS technologies
  - MITRE CVE[7] – a non-profit organisation providing Common Vulnerability and Exposures database and which has become the de facto standard for Information Security Vulnerability nomenclature
  - Law enforcement agencies - including police and specialist cybercrime units
  - Regulators – sector specific information.
- Specialised interest groups:
  - CERT UK CISP – Cyber Information Sharing Partnership[8] part of the UK's Computer Emergency Response Team
  - CPNI information exchanges – these information exchanges[9] share information primarily in relation to cyber-attack, and, depending on relevance to the purpose of the exchange, on vulnerabilities relating to physical and personnel-related threats.
- Commercial organisations:
  - Vendors are a primary source of information on new vulnerabilities found in their technologies. If required, the notification service should be made part of the maintenance contract with vendor organisations (hardware manufacturers, OS vendors, ICS solutions vendors, anti-malware companies)
  - Specialised vulnerability watch and threat intelligence organisations.
- Internal information sources:
  - Data from intrusion detection systems, firewall monitoring systems, system and network logs, anti-malware solutions and SIEM.
- Others:
  - Specialised press (e.g. technology magazines and publications)
  - Specialised forums and mailing lists (e.g. SCADA Sec).

[4] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems/at_download/fullReport

[5] https://www.cert.gov.uk/

[6] https://ics-cert.us-cert.gov/

[7] https://cve.mitre.org/

[8] https://www.cert.gov.uk/cisp/

[9] http://www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/

2.3 Identify vulnerabilities on the infrastructure

Using vulnerability assessment tools (e.g. data from intrusion detection systems, firewall monitoring systems, system and network logs, anti-malware solutions, SIEM) is another way to find current vulnerabilities existing in the ICS environment. A common method of vulnerability identification is through scanning however this should be conducted with care on ICS (see below).

In order to identify abnormal malicious activity, there needs to be a common understanding or a baseline of what normal looks like. With the help of staff who operate and manage the ICS, this baseline can be defined using various parameters including properties of network traffic, system resource usage, and time based events. This can be used to profile acceptable inputs, outputs and system behaviours associated with defined operation activities.

There are a number of key concerns to consider when using vulnerability assessment tools.

- It is necessary to ensure that all libraries and plugins associated with the selected tool are up to date with latest patch versions and are adapted to the type of technologies to be assessed.
- Assessing vulnerabilities in a live ICS environment should only be conducted with care as the use of active scanning may have unexpected consequences on the operations of the ICS. Active tools may aid in producing a comprehensive picture of a network however they may impact network bandwidth by introducing additional network traffic. This may introduce additional latency for operational communications and could in turn cause malfunctions to operational functions. Some ICS technologies (especially older technologies) are known to have little tolerance to unexpected traffic generated by these tools. Instances of outages due to malfunctions (and sometimes crashes) caused by security scanning have already been reported in the ICS community.
- Passive scanning tools are less likely to impact network bandwidth as they analyse existing traffic on the network without generating additional traffic. The network picture produced by these tools is generally less comprehensive than active methods as they can only analyse devices that are currently communicating with its monitoring points.

Vulnerability assessment should therefore be carefully considered, planned and authorised following an explicit risk assessment. An alternative to scanning live systems may be to use periods of planned shutdown (e.g. for maintenance purposes), or the use of a reference test platform that is kept up to date with the live configuration, or the maintenance spares. Limiting the throughput of scanning and having well trained specialists to control the scans are other safeguards that should also be employed.

Further guidance on vulnerability assessment in Industrial Control Systems can be found in the CPNI document ‘Cyber Security Assessments of Industrial Control Systems’[10].

[10] http://www.cpni.gov.uk/documents/publications/2011/2011008-infosec-cyber_security_assessment_of_ics_viewpoint.pdf?epslanguage=en-gb

3 ANALYSE IMPACTS AND REVIEW RESPONSE OPTIONS

New vulnerabilities or changes in threat activity constantly alter the risks organisations are exposed to through their ICS. In order to maintain an adequate and proportionate security posture, organisations need to adapt their strategy and solutions accordingly.

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

- On detection of new vulnerabilities or changes in the threat landscape, the potential impact for the ICS environment should be analysed. If there is an impact, potential response options like security patching should be explored. Where security patching is not possible or practical, compensating controls should be considered.

3.1 Analyse impacts

When information about new vulnerabilities or a change in threat landscape is identified, the first step is to assess its criticality. This may be in terms of the potential impact (e.g. the level of breach this vulnerability could lead to), ease of exploitation and level of activity of threat agents. This general evaluation can inform the speed of response required however this should not replace a specific evaluation of the associated risk in the given context of an organisation.

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

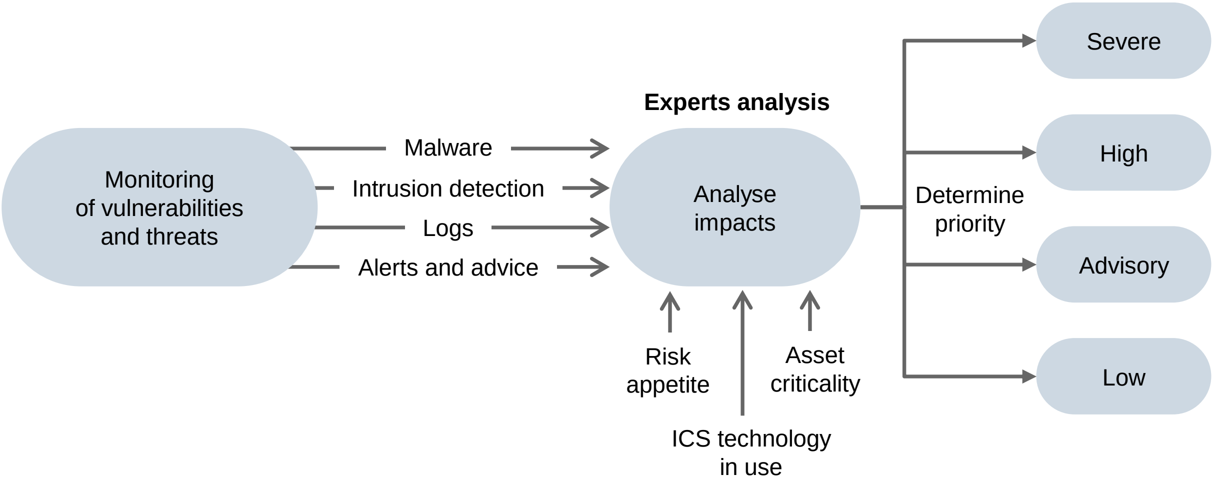
It is important to have personnel with the right expertise contributing to the analysis of security alerts, incident reports and information feeds. Although ICS are now often based on standard IT technologies, there are differences between the two environments. For example, personnel with networking skills and knowledge of application software may understand the general IT issues but not in the context of the ICS environment. Personnel with the relevant knowledge of those systems and their operational environment should also be involved.

Each alert needs to be assessed for the potential impact on the ICS in use and any appropriate action agreed. The assessment can be complex and any resulting analysis needs to be expressed in a clear and concise manner before being communicated to ICS SRT teams. One useful way is to categorise the information based on the threat (Figure 3) e.g.:

- **Severe** – a current incident or very high threat e.g. malware outbreak on the internet or on the enterprise or ICS network

- **High** – high threat vulnerability, e.g. significant external activity
- **Advisory** – low threat vulnerability at present that requires further monitoring e.g. activity on the internet
- **Low** – little direct threat to the ICS, e.g. E-mail malware where the e-mail function is not present on the ICS.

Figure 3 - Categorisation of ICS impact



Elements to consider when evaluating the risks associated with new vulnerabilities and threats:

- What is the actual impact of the vulnerability on the ICS systems (e.g. in terms of integrity, availability and confidentiality)? Can this vulnerability lead to impacts or malfunctions on the ICS environment? Recognise that this impact may vary in different areas of the system and this should be reflected in the priority given to actions.
- How can the vulnerability be exploited in the specific context of the organisation? Even if a system is vulnerable to specific attacks does not mean that the attack can affect all environments (e.g. if this uses protocols which are not allowed and are filtered on the network).

For more information on evaluating risks please refer to SICS Framework element ‘Manage the business risk’.

In order to simplify the decision making process, it can be useful to have agreed predefined criteria for each category of threat. However it should be noted that not all threats easily fit a predefined criteria. They need analysis by experienced IT and ICS specialists to interpret the available information and make appropriate decisions. Equally, as part of a defence in depth approach, it is always preferable to keep systems up to date with latest security patches. It is useful to base the priority / timing of patching on the criticality of the associated risks (e.g. emergency, high, advisory and low).

3.2 Review response options

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

Many ICS vendors require patches to be tested and accredited prior to deployment on live systems. Some vendors now automatically assess operating system patches as soon as they are released and provide advice on whether to deploy them. Where vendors are not automatically providing this then a specific request may need to be made for such an assessment.

In the past applying security patches to ICS was never a significant issue because these systems were based on proprietary technologies or isolated from other systems. Patches were only really required for system upgrades or for fixing bugs. Consequently application of these patches could usually be planned in an orderly installation process. However, patches are now essential as many ICS are now based on standard IT technologies, they are connected to other systems they run a risk of compromise or infection.

Applying protection measures such as firewalls to these systems is an important element of defence. However relying on a single strong layer of defence is no longer considered good practice for ICS protection and a multi-layer ‘defence in depth’ model is required. A critical element in such a model is to ensure that the devices located within the protection perimeter are hardened through a variety of measures – a key one being the timely application of security patches.

3.3 To patch or not to patch

When faced with a security alert or incident a key consideration is whether to deploy security patches or not. This decision should be largely driven from the risk assessment in the analyse stage. However, the application of patches is not risk free as there is a possibility that the patch might cause the incorrect operation of a system.

In addition, the effort and disruption of taking systems out of production to apply the patches needs to be weighed against the risk of not deploying them. Where possible, systems should be designed for ease of patching. Examples include:

- **Dual redundant servers:** allows one to be patched while the another maintains operations
- **Test or backup servers:** allows for the testing of patches before deployment to live systems.

These options need to be reviewed with the asset owner and the technical teams in order to select the most appropriate course of action.

4 TEST AND IMPLEMENT SELECTED RESPONSE

Patching or applying other protection measures constitutes a change to the operational environment. As with any change, it may introduce operational risks if not carefully planned and controlled.

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

- Implement processes for deployment of security patches to ICS. These processes should be supported by deployment and audit tools. The processes should make allowance for criticality assessment of patches, vendor certification of patches, testing of patches prior to deployment, and a staged deployment process to minimise the risk of disruption from the change. Ensure the security patching process can support patching in response to security alerts and incidents.

4.1 Develop a patching process

The response plan should contain a detailed patching process in order to provide a consistent and orderly approach to the deployment of system patches. There are a number of questions that should be considered in developing this process:

- What are the systems that might need to be patched (this can be obtained from the ICS inventory)?
- What is the ability to patch the systems?
  - vendor guidance and requirements
  - note it may not be possible to deploy patches to obsolete technology
- What are the patching priorities?
- How will patches be deployed?
  - Under business as usual situations
  - Emergency patch processes
- What patch deployment and audit tools are available and appropriate?
- What testing is required prior to deployment?
  - Is vendor accreditation required prior to patching systems?
  - Is site assurance testing on test rig or training systems possible?
  - Is it possible to patch some systems prior to vendor approval?
- Are there any assurance and deployment tools that could be used to assist the deployment process (these tools might require vendor accreditation prior to use)?

Answering these questions should help to define the test and deployment plan. The change then needs to be authorised through the change management process of the organisation. This should include provisions for dealing with emergency changes that may occur for particularly critical vulnerabilities and threat activities. Activities should include as a minimum:

- Sufficient testing before authorising the change
- A roll-back plan in order to get back to a previous known good state
- Updated configuration databases and asset registers
- Evaluation and agreement of all impacts of the change
- Updating of documentation

Further details on general patch management can be found in the CPNI guide, 'Good Practice Guide Patch Management'[11]. This guide is a general document and is not specific to ICS.

4.2 Mitigate the risk when you can't patch

Where patching cannot be implemented, compensating controls should be considered as an alternative which include:

- Replace or upgrade systems
- Physically isolate systems
- Segregate systems (e.g. by placing behind an appropriately configured firewall)
- Additional system hardening to block or limit the effects of the vulnerability
- Increase monitoring for signs of malicious activity
- Protect system with intrusion prevention systems.

In situations where the system cannot be patched and poses an unacceptable risk, the only alternative may be to cease using the system.

[11] http://www.cpni.gov.uk/Documents/Publications/2006/2006029-GPG_Patch_management.pdf

5 CASE STUDY: NU-CLEAR

5.1 Nu-Clear

Nu-Clear is a nuclear power generation organisation that operates several Evolutionary Power Reactors (EPR) worldwide, including the UK.

The EPR is designed with a number of passive and active protection measures including leak tight containment around the reactor and four independent emergency cooling systems, providing redundancy.

5.2 Monitoring the threat landscape

An existing vulnerability and threat management process existed in the company which monitored for information concerning ICS vulnerabilities and threat intelligence. The organisation was interested in any threat intelligence concerning the nuclear sector, the organisation and any of their key third parties. The sources of information used included:

- CPNI (monitor for threat information on state actors and terrorist)
- CISP & CERT-UK (monitor for alerts and any related incidents in other sectors)
- ICS-CERT (monitor for alerts of ICS vulnerabilities)
- Special interest mailing lists (monitor for new vulnerabilities and research activities)
- Commercial threat intelligence subscriptions (monitor for threat and vulnerability information)
- Open source (monitor for threat and vulnerability information e.g. anti-malware vendor reports)
- Third party arrangements (monitor for new vulnerabilities found in vendor products and incidents occurring in support organisations).

All relevant threat information received was assessed in terms of the impact on the organisation and whether or not it signified a change in the current understanding of the threat landscape. Any such change was reflected in the organisation’s risk register.

The company maintained an ICS inventory which included detail on the item build (hardware and software versions), date of when it was last maintained, and associated third party vendors. This inventory was used to cross reference any vulnerability information in order to identify the potential presence of known vulnerabilities on their systems.

During the last scheduled shut down for maintenance the ICS inventory was updated with any discrepancies found. It was identified that the emergency cooling system was using a Linux build based on Debian 6.0 instead of the recorded Debian 5.0. This discrepancy was updated in the ICS inventory.

5.3 Assessing the impacts and taking action

The following alert was received on a Wednesday morning from CERT-UK detailing a new vulnerability:

Name: CVE-2015-1234

Summary: Linux kernel privilege escalation affecting multiple Linux distributions

Description:

1. On 01/04/2015 a vulnerability was announced (ref CVE-2015-1234).
2. This vulnerability can be reliably exploited to escalate privileges and achieve kernel mode execution in a number of Linux distributions.
3. SMEP does not prevent arbitrary code execution; SMAP does prevent arbitrary code execution.
4. CVE-2015-1234 has a working patch for most distributions including:
    - Debian (versions 6 through 7)
    - Ubuntu (8.04 through 14.04)
    - Red Hat Enterprise (versions 5 through 7)
5. The real-world impact of this vulnerability depends greatly on the systems on which they are deployed.

The detailed description of the vulnerability highlighted that, if exploited, an unauthorised user with access to a system would be able to escalate their privileges and gain full root access. This would allow them to execute any command they wished. The site Single Point of Accountability (SPA) was contacted and the vulnerability was discussed further to identify the potential impact.

When assessed against the ICS inventory, it was identified that the only system vulnerable was the Debian based system operating the emergency cooling system. This was a safety critical system and would kick in if the primary cooling system were to fail. The primary cooling system however would not have been affected as it is based on a different operating system.

Further analysis of the vulnerability and the emergency cooling system highlighted that although the system was vulnerable, only someone with physical access to the system would be able to exploit it. Due to the standalone architecture implemented, it would not be possible for someone to gain remote access of the system.

It was assessed that, although the system vulnerable was a safety critical system, the vulnerability was relatively difficult to exploit therefore the overall criticality was assessed as advisory / medium.

- The response options considered were:
- Take the reactor offline and patch
- Keep the reactor online and patch
- Implement compensating security measures
- Do nothing

It was decided to keep the reactor online and patch the system. The system had quad redundancy therefore patching would take place on each part of the system in turn.

5.4 Rolling out the fix

The organisation contacted their vendor who provided them with a certified patch for the emergency cooling system. The patch was applied to a development machine with an identical build to the emergency cooling system. The machine was tested to ensure that the patch fixed the vulnerability and that it did not result in any adverse issues. After it was deemed that the patch was safe, it was installed on one of the redundant emergency cooling systems and subjected to further tests before being deployed on all of the affected systems.

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/