CESG

CPNI
Centre for the Protection
of National Infrastructure

SECURITY FOR INDUSTRIAL CONTROL SYSTEMS

ESTABLISH RESPONSE CAPABILITIES

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:	

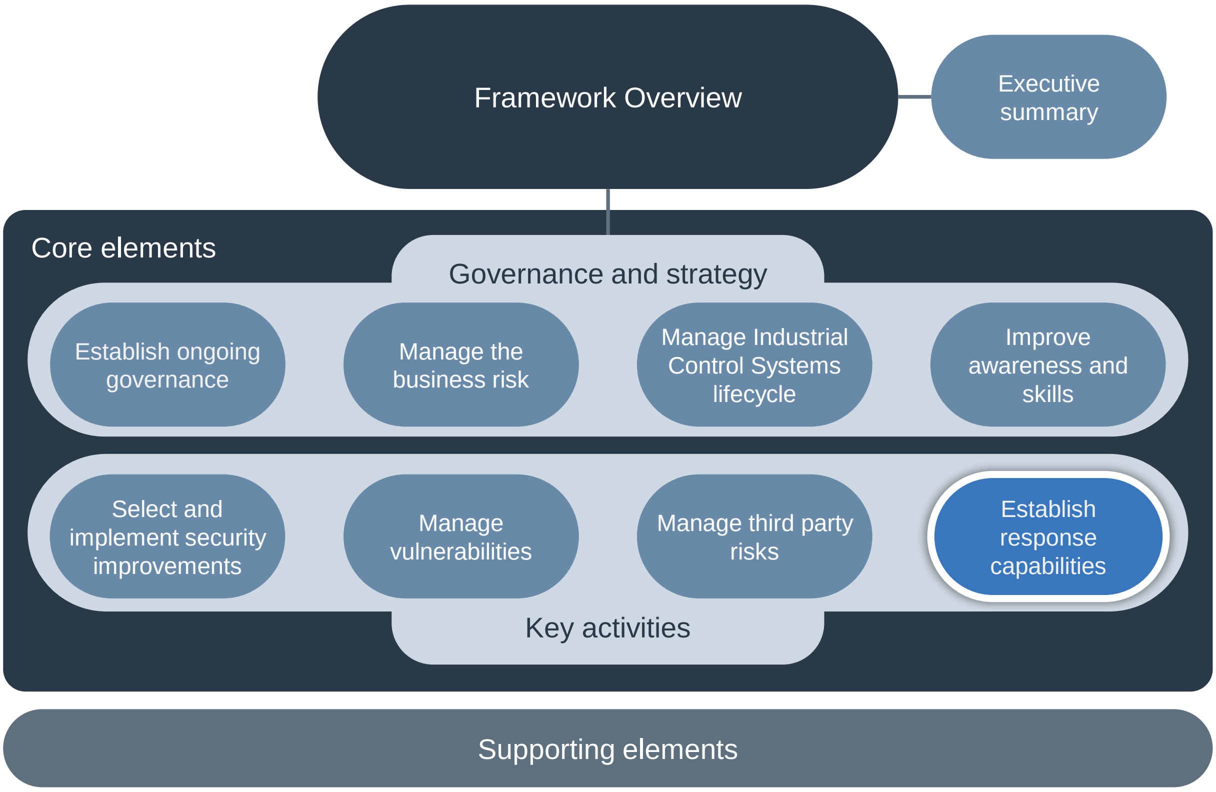
CONTENTS

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 guide fits in the SICS Framework



1.2 Establish response capabilities - summary

The objective of this guide is:

- To establish procedures necessary to monitor, evaluate and take appropriate action in response to a variety of cyber security events.

Organisations in the ICS environment will already have disaster recovery (DR) and business continuity plans (BCP) in place where DR focuses on recovering the systems that support critical business functions and BCP focuses on functions that support the business. However, due to the nature of the ICS technology and operational environment, these plans are often inadequate to deal with cyber attacks.

It is important to recognise that however good the security measures are, they cannot provide 100 per cent protection because both technical and non-technical vulnerabilities cannot ever be entirely eliminated. This means residual risks to systems will continue to exist and have to be managed alongside the need to identify and respond to any other changes in the threat landscape. An important aspect of effective management in this area is the identification of critical systems where the acceptable level of residual risk may be far less than for non-critical systems.

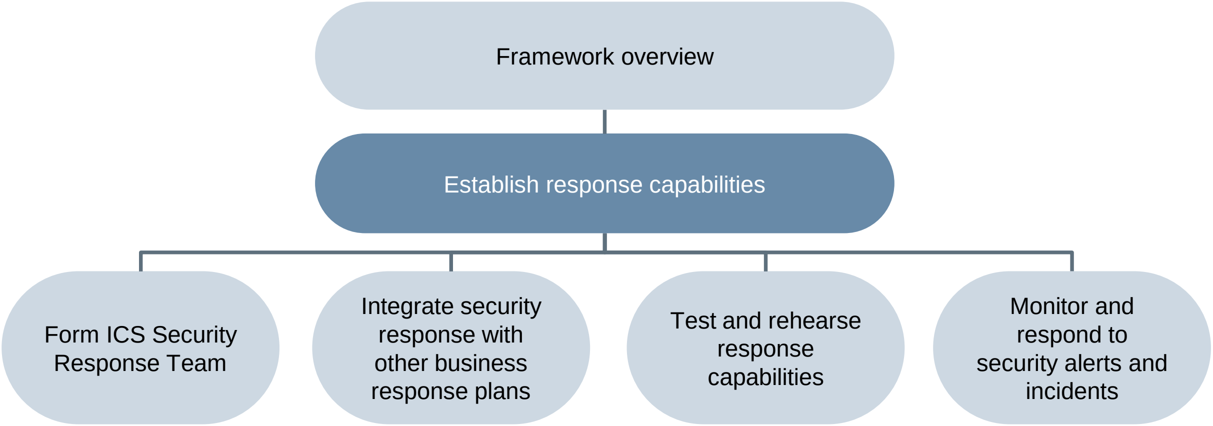
This good practice guide is aligned with the CPNI – First Responders' Guide on Incident Management which describes the target incident management process capabilities and provides guidance on how to establish capabilities for managing security incidents affecting ICS.

Analysis indicates that ICS security incidents from cyber attack were previously a rare occurrence and caused minimal disruption. While the number of proven attacks are still small relative to traditional threats to IT, they are now becoming more frequent[1] and organisations have to plan for them, both by revising their protective security regime and by developing or reviewing incident response policies and procedures.

Figure 2 sets out the four good practice principles that should be followed to establish response capabilities:

- Form an ICS security response team
- Integrate security response with business continuity plans
- Test and rehearse response capabilities
- Monitor and respond to security alerts and incidents.

Figure 2 – Good practice principles to establish response capabilities


Framework overview
Establish response capabilities
Form ICS Security Response Team
Integrate security response with other business response plans
Test and rehearse response capabilities
Monitor and respond to security alerts and incidents

[1] The ICS CERT Year In review report for 2013 shows a yearly increase of reported incidents of 41% from 2011 to 2012 and of 30% between 2012 and 2013.

2 FORM AN ICS SECURITY RESPONSE TEAM

Responding to security incidents in the ICS environment requires a team of specialists with the right set of skills who can be mobilised quickly in order to deal with situations that carry significant risks or are already causing disruption to operations.

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

- Form an ICS Security Response Team (ICS SRT) to respond to suspected security incidents. Representation should be drawn from a number of business areas including competent engineering staff familiar with ICS. A CNI company wishing to establish an ICS SRT can approach CERT-UK or CPNI for advice and support.

2.1 Create an ICS Security Response Team (ICS SRT)

An ICS Security Response Team (ICS SRT) is a core element of an organisation's response capability and provides the foundation for effective monitoring, analysis and management of alerts and incidents. The ICS SRT must be involved at every step in the process of monitoring an ICS situation, analysing any changes to the cyber threat and initiating appropriate responses. The ICS SRT should sit within the wider response team which typically covers other incidents relating to IT, and physical and personnel security.

A key requirement for a successful ICS SRT is to ensure that the right people with the appropriate knowledge and skills are involved. These skills may include network and malware analysis, and computer forensics. It may be necessary to seek and contract third party expertise in these areas if they do not exist within an organisation The team can either be part-time or full-time and may be a central, site or virtual resource. It is likely that many members of the ICS SRT will have these responsibilities in addition to their day to day responsibilities. Membership should be drawn from a variety of sources with representatives from a number of business areas, including:

- ICS teams
- IT security teams
- IT infrastructure
- Business management
- Operations
- Internal regulators
- Legal department
- Internal and external communication team

- Corporate media contact
- Corporate security team.

2.2 Organisational considerations

ICS SRTs can be structured in a number of ways, either centrally run, i.e. as part of a Security Operation Centre (SOC), or local site-run entities, or a combination of both.

In large organisations, it may be possible to have a central SOC that can monitor and analyse events, advising local sites on appropriate actions and co-ordinating their activities. A SOC can provide a better approach to incident response as it is usually ideally placed to share and obtain information from other groups such as business partners, vendors, other Incident Response Teams, law enforcement and infrastructure protection teams such as CPNI.

A SOC can also often provide an effective 24/7 operation, using fewer resources than a collection of individual local teams. However, a SOC also has disadvantages. For example, it may not have enough knowledge of the local sites to fully understand their operational environment or the people involved.

The alternative is a local site team that might be created using personnel who have a part time incident response role which is performed alongside their normal day to day activities. These teams will have extensive knowledge of local issues and operational environments. This approach is important at sites where the common response to particular incidents is to disconnect the ICS from the corporate network (where the SOC often resides), and this in turn disconnects the ICS from the SOC.

In practice, a hybrid approach is often preferable, i.e. a SOC sharing information with local teams based at the operational sites. This model leverages the efficiencies of a SOC in carrying out day to day monitoring, enabling the local site to concentrate on their normal core activities but respond to incidents or alerts when advised by the centre.

One of the major difficulties in this area, regardless of the preferred operational model, is the availability of personnel with the necessary operational, interpersonal, technical and incident management skills. Significant training may be required before a team can become fully effective.

Where incident response skills and training are issues for organisations, or when a particularly severe incident occurs that is beyond the capability of the local ICS SRT, an external government service is available to organisations on a commercial basis in the form of the CPNI/CESG Certified Incident Response Service[2].

[2] http://www.cesg.gov.uk/servicecatalogue/service_assurance/cir/Pages/Cyber-Incident-Response.aspx

3 INTEGRATE SECURITY RESPONSE WITH OTHER BUSINESS RESPONSE PLANS

Many organisations already have a variety of response and continuity plans in place. These include business continuity, disaster recovery, safety, health and environmental incident or other organisational and industry specific emergency plans supporting an overall crisis management capability. It is vital to security that plans adequately cover the variety of threats to ICS and interoperate satisfactorily.

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

- Ensure that appropriate cyber security response, business continuity, disaster recovery, and emergency plans are in operation for all ICS.
- Ensure that the cyber security response is integrated with other, business continuity, disaster recovery, and emergency responses.

3.1 Establish security response and continuity plans

It is rare for existing plans to adequately cover the variety of potential threats to ICS. This is because the threats, especially from cyber attack, were never really acknowledged when the plans were originally conceived. For example, if a disaster recovery system, installed to protect a control centre from physical incidents, is connected to the same network as the main control centre, then it is likely that a malware incident on the main system would also impact on the disaster recovery.

It may be possible to include cyber threat incident management within existing plans but care must be taken to ensure that all the appropriate ICS threats are adequately covered and that the various plans interoperate satisfactorily

There can also often be confusion around how incident response, disaster recovery and business continuity planning fits together. Some definitions of those different plans are set out below:

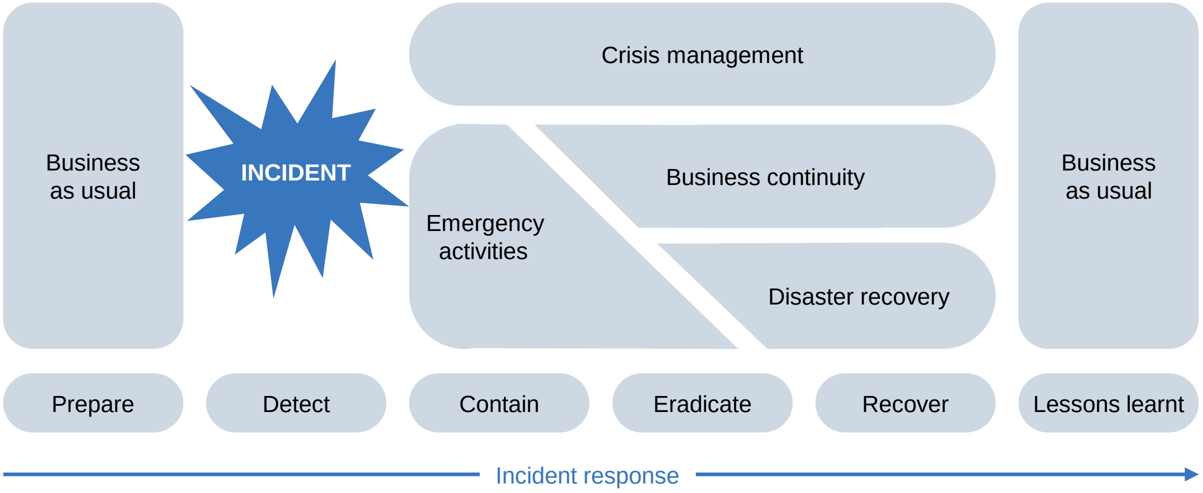
- **Incident response**: In the context of ICS security, and in the CPNI Good Practice Guides, incident response relates to all the activities linked to the management of security incidents affecting ICS environments. As described in CPNI First Responders Guide[3], this covers six main steps: Prepare > Detect > Contain > Eradicate > Recover > Lessons Learnt, see Figure 3

[3] http://www.cpni.gov.uk/Documents/Publications/2007/2007011-First_responders_guide.pdf

- **Emergency plans**: These are activated upon detection of an emergency. They are designed to take emergency measures in order to provide essential safety and security measures to limit the impact of the incident. There are different kinds of emergency plans in organisations, for example: Health, Safety and Environment emergency plans with detailed responses to specific events (e.g. fire, accidental release of chemicals), IT emergency plans and ICS emergency plans which aim to contain the effect of an ongoing incident or preserve evidence for forensics purposes. They are activated during the "Contain" stage of incident response.
- **Business Continuity Plans:** These are developed by the business to help maintain a desired minimum level of activity following an adverse event. Different plans are usually built for different scenarios of incident or disaster (some ICS related and some related to other types of scenarios – e.g. pandemics). They rely on a mix of business fall-back procedures, use of alternate working and production facilities and on IT and ICS Disaster Recovery capabilities.
- **Disaster recovery plans:** These apply generally to facilities and technology such as IT or sometimes ICS. Those plans utilise the organisation's capabilities to recover from incidents and disasters: they rely on backup facilities and technology that can be activated at short notice within the timeframes and level of service agreed with the business users. They also cover reconstruction activities which aim to rebuild the nominal capabilities. Resilience measures are often designed into ICS to aid disaster recovery, for example where backup facilities are not available, they use redundant technologies to support isolation and restoration during incidents, and diverse technologies to minimise impact.
- **Crisis Management Plans**: Crisis management is a wider concept that applies to organisations as a whole. The associated plans usually cover a wide range of situations and should include ICS security incidents. The primary purpose of these plans is to ensure that the organisation operates through an effective chain of command, that situational awareness is maintained at the different levels of an organisation and that communication (internal and external) is managed consistently.

These different concepts do not operate in isolation and are interdependent. An illustration of how they interact is provided below in Figure 3.

Figure 3 – Different types of response plan



The figure shows how incident response spans across all the steps from preparation to lessons learnt and how emergency plans focus on the short period of time directly following an incident and provide an immediate response. As incidents progress, the focus shifts to initiating business continuity (ensuring the business can continue to operate during the incident) and disaster recovery (restoration of lost or damaged data and systems). Crisis management covers all coordination across the organisation and with external stakeholders, from detection to return to business as usual. Not all cyber security incidents trigger all the response plans, for example some security incidents may not have direct operational impact and therefore would not trigger business continuity and disaster recovery but would still need to go through the contain, eradicate, recover, lessons learnt process.

In establishing effective response plans for ICS systems, there must be a focus on incident response, as digital security events often occur suddenly without notice and require rapid and effective action in order to avoid incidents or minimise their impact if they cannot be avoided.

3.2 Key contents of a response plan

ICS security response plans are often quite wide-ranging and must be drafted in accordance with the chosen operational model, e.g. as a SOC or local site, however as a minimum they should include:

- Procedures for reporting incidents
- Processes for invoking the response plan and, in particular, qualification criteria to determine whether it is a cyber security incident
- Details of the response team personnel, their deputies, roles and responsibilities and full 24/7 contact details
- Critical sites, systems and assets to the business
- Predefined procedures to possible scenarios as previously identified
  - A clear definition of how to identify each scenario
  - A clear action plan in the event of a scenario being identified as in progress
- A clear escalation path, and authorisation requirements for escalation
- Lists of supporting tools available
- Contact information (including internal and external agencies, companies, law enforcement, vendors etc.)
- A clear communication plan
  - How to communicate
  - What to communicate
  - To whom
- When to communicate and how often
- The criteria to be met in order to close out incidents.

4 TEST AND REHEARSE RESPONSE CAPABILITIES

Real incidents have shown that response plans are significantly less effective if they are not tested or rehearsed before being invoked. Those tests and rehearsals verify that the provisions in the plans are appropriate and that personnel know the plans, and their respective roles and responsibilities. Additionally it is important to ensure that duplicated facilities and assets that support the response plans are maintained so that they work when required.

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

- Ensure that all cyber security plans are regularly maintained, rehearsed and tested.

4.1 Ensure plans are regularly maintained, rehearsed and tested

Even with careful planning, it is often found that plans and personnel behave differently in real life situations. So all relevant personnel should be trained in the execution of the plans and these should be regularly tested to ensure that they perform in the manner they were designed for.

This topic is covered further in the 'Improve awareness and skills' element of the SICS Framework.

A range of different test and rehearsal techniques can be used:

- Call tree: this type of test will verify that the alert, communication and mobilisation process of the response plans are effective. It should cover the different communication methods which are used as part of the response plans. Loss of availability of some means of communication or key participants can also be introduced in the exercise.
- Walk through: this is a peer review where the response plans are reviewed for completeness and accuracy. These reviews are particularly effective when conducted with stakeholders representing different areas of the business and who are therefore able to offer an understanding of the wider business priorities and processes.
- Table top exercises: these are useful to simulate the execution of the response plan, based on a fictitious scenario. These tests are usually very efficient at testing the communication, the decision making process, the coordination of the strategy and at raising the awareness of participants towards the kind of mind set they need in managing incident response.
- Technical tests: these range from the simple testing of an individual system restoration procedure to full activation of DR facilities in parallel or in lieu of primary facilities. More representative types of tests transfer production to the DR environment but these bring very substantial risks and should

be carefully planned and subject to a formal risk assessment. It might be more practical to simulate activation of DR using a restricted aspect of the ICS (e.g. backup control room).

Plans should be reviewed at least annually and more frequently for critical or high-risk systems. They should be modified following any changes to the threat or protective security requirement, the system itself or organisational structure. Lessons learnt during an exercise or following incidents should also be incorporated into the plans.

5 MONITOR AND RESPOND TO SECURITY ALERTS AND INCIDENTS

Managing ICS security incidents requires a number of essential steps to build associated capabilities in monitoring, analysis and response.

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

- Establish an early warning system that notifies appropriate personnel of security alerts and incidents.
- Establish processes and procedures to monitor, assess and initiate responses to security alerts and incidents. Possible responses may include: increase vigilance, isolate system, apply patches, or mobilise the ICS SRT.
- Ensure all ICS security incidents are formally reported and reviewed and that lessons learnt are captured and fed back in to the incident response process.

5.1 Establish an early warning system

Having a well defined and rehearsed early warning system will enable organisations to respond rapidly and effectively to security alerts and incidents, minimising their cost and disruption.

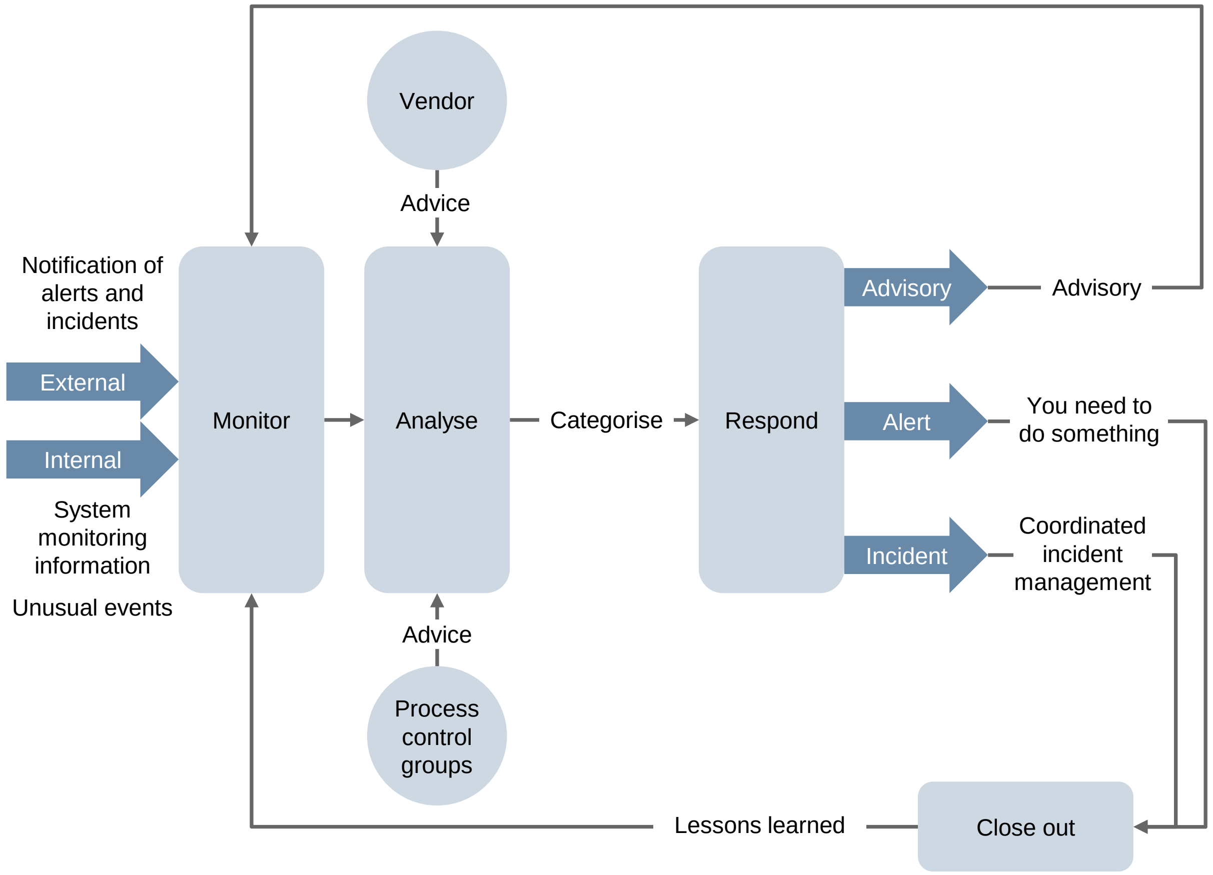
Many organisations have response and continuity plans in place but often they are not effective at identifying security incidents, determining the appropriate action and initiating the response plans.

A common problem is that organisations do not have timely access to actionable information from internal and external sources on which to base decisions. Another issue is that they can be overwhelmed by a large volume of information that they cannot effectively process as it obscures the relatively small amount of actionable information relating to the incident. This lack of an effective and well resourced analytical capability leaves organisations unsure of the problem and how to react to it.

To address these issues, a high level incident triage process is needed. An example is outlined in Figure 4 which sets out three key stages involved in responding to events.

- **Monitor** – collect information security data from inside and outside the organisation, such as alerts, virus infections, threats, patch notifications, incident notifications and data from network and performance monitoring systems.
- **Analyse** – categorise the information received from the various sources into different levels and types of potential threat in order to determine whether a response is required. This analysis should take into account the criticality of systems and acceptable operating thresholds that, if exceeded, will trigger an alert.
- **Respond** – work out how to respond based on the type and category of threat and the associated risk to the organisation.

Figure 4 – ICS security response overview



5.1.1 Monitoring stage

The normal state of operations is where both internal and external information feeds are monitored for any relevant events. These will be abnormal system behaviour or alerts gathered through the vulnerability management process (see SICS Framework element 'Manage vulnerabilities').

Internal Monitoring

General system monitoring of reliability events and failures such as system uptime on ICS is considered normal business practice. However, additional security monitoring of activity on the systems is often mistakenly considered to be time consuming and to require additional work. This need not be the case and organisations should extend the set of monitored data to include these security events. Depending on the criticality of the systems, organisations should choose an appropriate frequency for proactive monitoring (that can be modulated depending on the perceived threat level) and mechanisms for triggering ad hoc log analysis of logs and monitoring when there is suspicion of malicious activities taking place.

Security monitoring and log analysis is performed using a number of information feeds from:

- Firewall monitoring systems
- Security incident and event monitoring systems (SIEMs)
- Intrusion detection systems
- System and network performance monitoring systems
- System fault reports.

Those activities can be facilitated through the use of log correlation and analysis tools. SIEM tools provide capabilities for managing large numbers of logs and alerts, however compatibility between ICS solutions and such tools needs to be carefully considered before choosing these solutions.

External Monitoring

Using external information as part of the monitoring is a key to establishing an effective early warning system. External sources of information include:

- Computer Emergency Response Teams (CERTs)
- Specialised interest groups
- Commercial organisations.

More information on external data sources can be found in the SICS Framework element "Managing vulnerabilities".

It is envisaged that, in the near future, security monitoring data will be combined with process monitoring data to correlate process variable boundary limits with security events. The aggregation of different data types should enhance security monitoring on ICS.

5.1.2 Analyse stage

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 new piece of malware represents a problem to the organisation when it may have infected systems far sooner. This can be a difficult task but there are tools available that are specifically designed to provide more efficient analysis of this information.

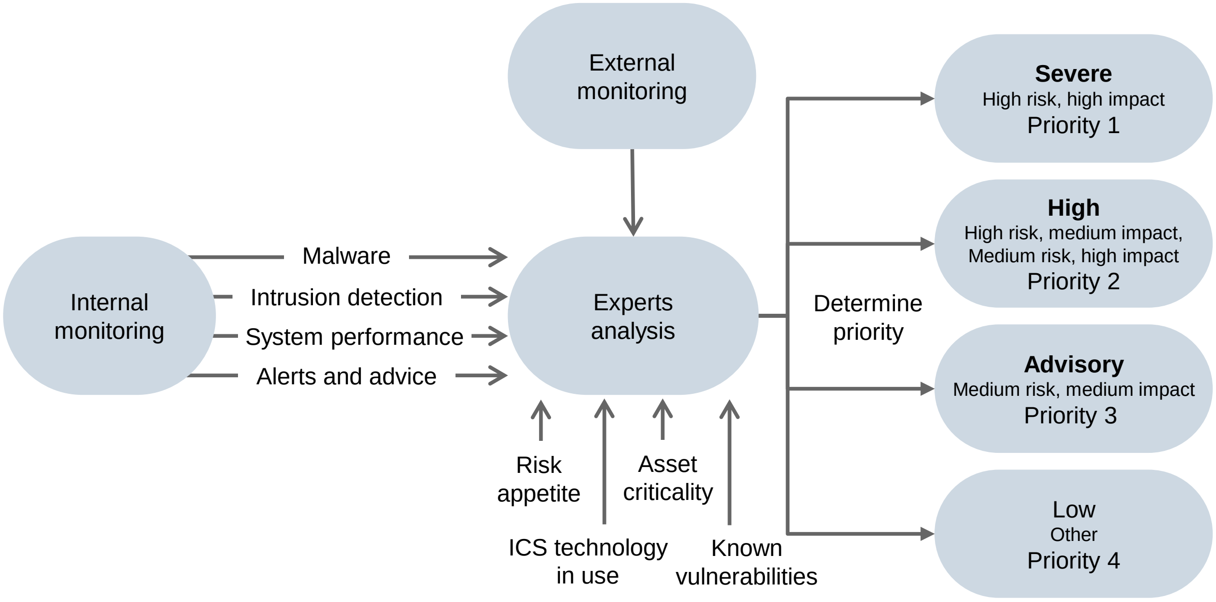
It is important to have personnel with the right expertise contributing to the analysis of security alerts, incident reports and information feeds. Although control systems are now often based on standard IT technologies, there are differences between the two environments. For example, personnel with networking skills and knowledge of application software will be able to understand the general IT issues but in the ICS environment personnel with the relevant knowledge of those systems must also be involved.

Each alert needs to be assessed for the potential impact on the ICS systems 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 5) e.g.:

- **Severe** – a current incident or very high threat e.g. malware outbreak on the internet or on the corporate or ICS network
- **High** – high threat vulnerability, e.g. important external activity
- **Advisory** – low threat vulnerability at present further monitoring is required, e.g. activity on the internet
- **Low** – little direct threat to the control system, e.g. E-mail virus where the function is not present on the ICS.

In order to simplify the decision making process it can be useful to have agreed predefined criteria for each category. It should be noted that not all threats will easily fit a predefined criteria. Such threats will need the experienced analysis of IT and ICS specialists to interpret the available information and make appropriate decisions.

Figure 5 – Categorisation of ICS security threat data



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

Further guidance is provided in SICS Framework element 'Manage vulnerabilities'.

5.1.3 Respond stage

This stage is about initiating the appropriate response to an incident in a timely manner to avoid further unnecessary exposure and should be part of the response team's objectives. The trigger will normally be the results of the previous analysis stage. Typical situations are:

- Security alert (e.g. advance warning of a possible incident, increased hacker activity or possible malware problem)
- Vulnerability notification (e.g. a vulnerability has been identified or a software patch has been released for a control system)
- Malware infection (e.g. virus is detected in a control system)
- Hacker compromising an ICS.

5.2 Establish processes and procedures

Examples of what should be considered when preparing a response plan can be found in the CPNI's First Responders' Guide Policy and Principles[4].

The procedures included in an ICS response plan need to take into consideration the operational environment, potential threats, vulnerabilities and experiences from previous incidents. The following are some procedures that could be included:

- Malware infection and removal
- Forensic capture and analysis (live systems and images)
- Suspected hacker infiltration
- Denial of service (DoS) attack

[4] http://www.cpni.gov.uk/Documents/Publications/2007/2007011-First_responders_guide.pdf

- Disconnection of control system from other networks (if possible)
- Reconnection of control system to other networks
- Inability to view status of plant (loss of view)
- Inability to control the plant (loss of control)
- Emergency anti-virus and intrusion detection system signature updates
- Business as usual and emergency security patching processes
- System backup and restore
- Confirmation of correct system operation (i.e. a procedure for verifying that a system is operating as normal and there are no signs of secondary malware infection).

The following sections examine considerations for the use of system forensics. Additional guidance on vulnerability and patch management can be found in SICS Framework element 'Manage vulnerabilities'.

5.2.1 System forensics

Where the system has been compromised (e.g. by malware or a hacker) there is often a difficult decision to make as to whether to restore a system or keep it quarantined for further investigation so the attackers can be pursued. There is usually a pressing need to restore the systems to an operational state as quickly as possible, which usually involves its rebuilding or restoration using backups. Unfortunately this often means that any clues or audit trail left by the attacker is destroyed and therefore there will be little chance that the perpetrator can be pursued and brought to justice. This type of dilemma can be addressed by designing, implementing and operating a "forensics ready" infrastructure that would ensure that:

- System event and security logs are exported to a secure repository so that reliable logs can be analysed even if the impacted systems are down, or have been restored and their previous logs lost,
- A rapid forensics capability can be deployed with:
  - Documented procedures to quickly and effectively collect evidence (any errors in implementing the procedures can be irreversible and lead to loss of evidence)
  - Specialised skills (internal or external) to conduct forensics activity
  - Specific equipment to copy data without altering the impacting systems and preserving the chain of evidence.
  - All these aspects need to reflect the local legal constraints of the country where the systems are located as specific additional requirements can exist (e.g. need to have a legally recognised third party to oversee forensics activities for evidence to be admissible in a court of law).

Forensic investigation of retained logs and disc images can be complex and is normally beyond the capability of typical organisations. It is usual to obtain specialist support under a commercial arrangement from external companies. These investigative services are important in establishing a time line of events during the compromise. This may help to uncover what was done, how it was done and potentially by whom. This will help in providing the evidential basis for any prosecutions and will require sufficient detail to prevent any reoccurrence. This topic is a specialist area in itself; and further information is available in the CPNI document 'An Introduction to Forensic Readiness Planning'[5].

5.2.2 Establish incident reporting

There is a strong tendency for ICS security incidents to be kept confidential and for organisations not to disclose incident information to external agencies in order to protect reputation and to discourage external scrutiny.

[5] http://www.cpni.gov.uk/Documents/Publications/2005/2005008-TN1005_Forensic_readiness_planning.pdf

However, there are advantages to sharing information about incidents. It can allow further investigation by other agencies, the avoidance of similar incidents in other organisations, and the sharing of experience and remediation measures between organisations to develop a better understanding of the risks facing control systems.

Any organisations that have experienced ICS security incidents are strongly encouraged to share this information (in an appropriate manner e.g. anonymously) with CPNI. There is a mechanism to do this through the Cyber-security Information Sharing Partnership (CiSP),[6] which is part of CERT-UK.

This is a joint industry and government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness and therefore reduce the impact on UK business. It allows members from across sectors and organisations to exchange cyber threat information in real time, in a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information.

CiSP members receive enriched cyber threat and vulnerability information from the ‘Fusion Cell’, a joint industry and government analytical team who examine, analyse and feedback cyber information from a wide variety of data sources. This ultimately adds value to CiSP members and helps organisations at all levels of cyber maturity. The Fusion Cell also provides a range of products and services, including alerts and advisories, weekly and monthly summaries, as well as a capability to conduct bespoke malware and phishing email analysis on behalf of CiSP members.

5.2.3 Ensure lessons are learnt from incidents

It is important to ensure that, following situations where a response to a digital security alert or incident has been required, any lessons or possible improvements to the process are identified and acted upon to ensure continuous improvement of the response processes.

Post incident reviews should be carried out both centrally and locally and could trigger updates to response plans, policy and standards and the enterprise risk profile. This activity can be enhanced where infrastructure exists for replaying or recreating the incident.

This is one of the inputs into the continuous improvement process described in the ‘Establish Ongoing Governance’ and ‘Manage the Business Risk’ element of the SICS Framework.

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

6 CASE STUDY: MAJOR OIL & GAS

6.1 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.

Following the successful work to remediate ICS security risks, the organisation recognised that their existing Disaster Recovery (DR) and Business Continuity Plans (BCP) did not cover ICS. Having carried out some investigation the organisation discovered that site responses to ICS security incidents were variable and reactive, resulting in sites taking a long time to return to normal operations.

6.2 Forming an ICS Security Response Team (ICS SRT)

Having recognised the need for a specialist ICS response, the organisation created a team dedicated to ICS incidents to sit within their existing incident response team. The team was responsible for monitoring, analysing and managing the response to any ICS incident. Each site was then accountable for carrying out the remediation and mitigation needed and reporting their progress back to the ICS SRT.

This team was made up of the following key personnel:

- For each of the main business areas(exploration, production, refining, distribution and petrochemicals) the following were included:
  - Senior Technical Authority for ICS
  - Senior Operations Manager
  - Head of IT
- CISO
- Head of Cyber Threat and Security Operations Centre.

This team was complemented by personnel from the existing incident response team to cover internal and external communications, legal aspects and wider contacts within the organisation.

6.3 Creating and testing response plans

The organisation created a small project team to support the sites in developing the response plans, spread good practice between the sites and look for ways to improve the plans. A decision was made to create an ICS Response Plan template that each site would complete to ensure a consistent approach and that the appropriate areas were covered.

The project team identified the personnel at each site who were necessary to providing the input for the plan, reviewing the procedures and signing it off. A series of workshops, often virtual due to the dispersed nature of the organisation's sites, were held to develop the content. These workshops identified any procedures that needed to be developed and defined roles and responsibilities during an incident.

Having completed the plans the next stage was to test them. The project identified three different types of tests:

- Communication testing
- Scenario table top exercises
- Technical testing.

Having completed testing, plans were updated, reviewed and signed off.

A key lesson learnt from this exercise was that carrying out technical testing was difficult when it involved the live system due to a fear of creating an incident during the testing. Opportunities to test on the live system were further limited as during shutdown periods the staff who were needed to carry out the testing were involved in maintenance activities.

6.4 Monitoring and responding to security alerts and incidents

In addition to creating the ICS SRT a decision was made to expand the role of the Security Operations Centre (SOC) to cover monitoring during ICS incidents. The SOC had two objectives:

- Monitoring of events and alerts to provide early identification of issues
- Providing the ICS community with support during an incident.

The SOC's revised role included internal monitoring of networks, firewalls and systems and external monitoring of events relevant to the ICS community. The next stage was to analyse these events and provide the sites with a summary of the alert with a severity rating. During an incident the SOC was to provide advice to the site about potential mitigation actions they could undertake and provide specialist support for any issues raised.

6.5 Benefits to the Organisation

Not long after the sites had created their incident response plans a major vulnerability was discovered in the core operating system used by over 90% of the systems in the organisation.

Each site was able to invoke their plan and, with the support of the SOC, implement the required mitigation without impacting the ICS. During a lessons learnt follow up a number of areas of improvement were identified in the SOC, including communication. There was an overreliance on e-mail leading to delays where a phone call may have been more appropriate. Each site reviewed their response and updated their plans accordingly.

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/

NATIONAL
SECURITY
ARCHIVE

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu