Rail Cyber Security
Guidance to Industry

February 2016

The Department for Transport has actively considered the needs of blind and partially sighted people in accessing this document. The text may be freely downloaded and translated by individuals or organisations for conversion into other accessible formats. If you have other needs in this regard please contact the Department.

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 0300 330 3000
General enquiries https://forms.dft.gov.uk
Website www.gov.uk/dft

Contents

Foreword

Cyber security is concerned with the security of cyberspace, which encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks. For the purposes of the rail industry, the scope of this guidance is any cyber system that is used to operate the railway particularly where safety and/or reliability are important.

This guidance document is designed to support the rail industry in reducing its vulnerability to cyber attack. It is designed to be high-level. It sets out the principles and general approach to cyber security, as good practice. It does not provide detailed instruction.

The guidance has a particular, but not exclusive, focus on protecting infrastructure and rolling-stock systems. It incorporates bespoke advice for railway-specific systems, as well as more general advice, to form a complete approach.

It is not designed to be used as a technical manual, Code of Practice (CoP), regulation or statutory instrument.

Its principles can also be utilised across the regulated and unregulated light rail networks.

It can be used to:

- inform and guide your senior management team
- support effective cyber security policy in your organisation
- raise awareness of cyber security in your organisation

It has been written with three specific objectives in mind:

- to support you in managing the overall risk of a successful cyber attack on your organisation's systems and operations.
- to support you in encouraging suppliers and maintainers, contractors and sub-contractors to ensure that appropriate defences and resilience against cyber attacks are built into the systems and products they supply.
- to support development of further documentation on cyber security, including further guidance and industry-developed detailed operational guidance.

Following this guidance will help you to strengthen your cyber systems against deliberate and non-deliberate attack.

1. Overview

Cyber attack poses a growing threat to the security and therefore the safety of infrastructure in Great Britain, including the railway networks. The threat is evolving. Expert opinion and research suggests that cyber systems are likely to contain vulnerabilities through insufficient protection.

The Government is committed to reducing the risk to the UK posed by cyber attack, by working in partnership with industry. It has made the following statement about cyber security and the partnership required to deliver it for the UK:

'Though the scale of the challenge requires strong national leadership, Government cannot act alone. It must recognise the limits of its competence in cyberspace. Much of the infrastructure we need to protect is owned and operated by the private sector. The expertise and innovation required to keep pace with the threat will be business-driven.

Similarly, though we can improve our defences domestically, the internet is fundamentally transnational. Threats are cross-border. Not all the infrastructure on which we rely is UK-based. So the UK cannot make all the progress it needs to on its own. We will seek partnership with other countries that share our views, and reach out where we can to those who do not.'

The UK Cyber Security Strategy – Protecting and Promoting the UK in a Digital World

November 2011

Rail operators have obligations under EU and domestic law to protect the safety of their operations. Failure to take reasonable care to do so may make them liable for some of the resulting losses.

1.1 The Department for Transport (DfT) gives binding counter terrorist and security instructions to station and passenger train operators in Great Britain, using its powers under the Railways Act 1993, to reduce the risk of a terrorist incident including the possibility of a cyber attack triggering widespread disruption, destruction or even loss of life. DfT also has equivalent powers under the Channel Tunnel (Security) Order 1994 (CTSO) to protect the Channel Tunnel and its users from acts of violence. In addition DfT provides guidance on other security related topics, such as designing security into stations, recruitment of staff, training and contingency planning. We also publicise within the transport sector security guidance from specialised agencies of government.

1.2 DfT's approach to the cyber threat is to rely firstly, on the existing combination of general safety and security obligations (e.g. access restrictions), guidance and security awareness. This document provides comprehensive additional guidance to support the specific requirements of the rail network and to mitigate threats posed by both terrorist and non-terrorist hostile actors.

Role of government

Government can support industry by:

- advising on the nature of the threat, both in general terms (industry forums) and through specific updates (direct communication with designated contacts)
- helping to share best practice through supporting and informing networks
- assisting industry and operators who are faced with attack
- defining the cyber security goals and expectations necessary for the protection of public safety and the critical infrastructure
- speaking for the UK in international fora (e.g. the European Union), as necessary, to help create an environment in which security is given a higher priority and designed in at the concept stage and there are common protocols to guide and assist defence.
- assisting in the response to incidents.

Governance

1.3 DfT has the task of giving instructions and overseeing rail security on the GB rail network. As far as the Channel Tunnel is concerned, it shares this responsibility with the French Government. DfT is the owner of government policy for cyber security for the rail networks, as explained in this document. This guidance is jointly governed by DfT as its primary author, and the Rail Safety and Standards Board (RSSB), as its host and primary editor, through the High Integrity System Group (HISG)

1.4 Effective cyber security is reliant on full engagement at all levels of an organisation. This level of engagement requires management boards to set a cyber security strategy for their organisations and ensure they are delivered. Good practice can include the appointing of a board champion with a specific responsibility to drive the necessary working culture to support the policy. RSSB will take forward development of voluntary standards, for specifying the level of security required by a security management function.

1.5 Middle and front line management are also key in delivering effective cyber security by ensuring that their company's cyber strategy is delivered through working practices.

1.6 In the event of an incident taking place, DfT and other parts of government may hold some governance over the incident handling dependent on the size and nature of the event. These arrangements are outlined in Section 3 – Handling Threats and Incidents.

See:

- Process Control and SCADA Security Guide 7 - Establish Ongoing Governance (cpni.gov.uk)
- ISA62443 (Isa99.isa.org)

1.7 Government has implemented a framework specifically to ensure that these actions can be undertaken. The framework includes:

- an assessment capability in government that can provide an authoritative assessment of the cyber threat and cyber security issues.
- **the Computer Emergency Response Team for the UK (CERT-UK)**. This provides a monitoring, response and coordination function for cyber security at a national level. CERT-UK will coordinate cyber incident response across all public and private sectors. CERT-UK (cert.gov.uk)
- **the Cyber Security Information Sharing Partnership (CISP)**. This is an initiative hosted by CERT-UK to bring together industry to share good practice and information on incidents in a confidential environment.

1.8 More broadly, the government is looking to encourage use of the US National Institute of Standards and Technology (NIST) cyber security framework amongst UK companies that operate critical infrastructure (especially where an appropriate, alternative approach is not in place). The framework provides a means of understanding and managing cyber security risks in an organisation, is non-regulatory in its approach and we will be looking to discuss UK industry input to its development going forward.

1.9 In addition, the Department for Business, Innovation and Skills' (BIS) Cyber Essentials scheme is a government-backed, industry supported initiative to help organisations protect themselves against the most common types of cyber-attacks – this may be of particular use to companies looking to help secure their supply chain as it provides a basic accreditation that suppliers can adopt. Further information on DfT and wider government's position on standards and best practice (and the support available) will be forthcoming.

See:

- National Institute of Standards and Technology (NIST) cyber security framework (nist.gov)
- BIS Cyber Essentials (gov.uk)
- HM Government Security Policy Framework (gov.uk)

Using the guidance

What this guidance applies to

1.10 This guidance can apply to all rail networks in Great Britain. Its primary audience is:

- the high-speed heavy rail network
- the conventional heavy rail network
- the London Underground network
- the Docklands Light Railway
- the Glasgow Subway

However it can also be followed on unregulated scenic and heritage networks where rolling-stock runs on Network Rail operated tracks and on the light rail and tram networks.

Who this guidance applies to

1.11 This guidance applies primarily to all rolling stock and infrastructure owners and operators and manufacturers. It is also applicable to suppliers, subcontractors and maintenance contractors on the GB rail network, who will need to be aware of changing expectations in the industry that they are supporting. It is designed to provide guidance towards delivering a level of cost effective protection against cyber attack, in line with the As Low As Reasonably Practicable (ALARP) principle as it relates specifically to effort made towards the mitigation of threats and vulnerabilities. Its key audience in each organisation is those with overarching responsibility for cyber security. However, there are also important messages for corporate management who are responsible for setting cyber security strategy, managing enterprise level risk, and providing the mandate for cyber risk owners to act.

1.12 There are particular parts of the guidance that will be applicable to other members of your organisations.

How to use this guidance

1.13 Following this guidance will help you to strengthen your cyber systems against deliberate and non-deliberate attack, reassure your passengers, staff and the general public and increase confidence in the security of rail networks.

1.14 This guidance is designed to be high-level. It sets out the principles and general approach to cyber security as good practice but does not provide detailed instruction at a technical level for engineering or operational staff (although in places we have provided links to existing generic technical guidance and standards)

Recommendation for future work

1.15 DfT recommends the development of detailed operational guidance by industry including detailed requirements, measures and voluntary standards. DfT consider that industry is best placed to develop this guidance on a ‘for industry, by industry’ basis – through the RSSB. With this in mind, it will be for industry to implement, monitor and update it as necessary.

The threats

Cyber technology is complex and fast evolving, and cyber attacks are becoming increasingly automated and sophisticated.

Railway systems are becoming vulnerable to cyber attack due to the move away from bespoke stand-alone systems to open-platform, standardised equipment built using Commercial Off The Shelf (COTS) components, and increasing use of networked control and automation systems that can be accessed remotely via public and private networks.

The threat of cyber attack arises from organisations and people referred to as hostile actors. Their exact intentions are wide and varied, ranging from the desire to cause death, through to the desire to cause minor disruption, inflict reputational damage or steal data.

There are also threats posed by employees operating systems inappropriately, and from inertia within the supply chain regarding the introduction of cyber security measures to engineering systems.

The modes of attack

1.16 Cyber systems used on GB rail networks may be subject to unauthorised access through various means:

- remotely, via the Internet, or unsecured telecom networks.
- at close hand, through direct contact with infrastructure (e.g. through a USB port).
- locally, through unauthorised access to physical infrastructure, or insider threat (infiltration).

The vulnerabilities

1.17 Vulnerabilities are weaknesses in control systems, information systems, system procedures, controls, or implementations that can be exploited by a threat source.

1.18 Vulnerabilities can result from many sources, including:

- policy and procedure
- architecture and design
- configuration and maintenance
- physical intrusion
- software development
- communication and network
- lack of training and awareness

See:

- Guide to Industrial Control Systems Security (csrc.nist.gov)
- 20 Critical Controls for Cyber Defence (cpni.gov.uk)
- Configuring and Managing Remote Access for Industrial Control Systems (cpni.gov.uk)
- Remote Access for ICS (cpni.gov.uk)

1.19 Evidence derived from government-funded research, demonstrates that there is some good cyber security provision in the rail industry, but that provision is variable. This means that vulnerabilities exist. Further to this point, there is a lack of cohesiveness in the industry meaning that cyber security regimes are developed in isolation, exacerbating the uneven provision and creating vulnerabilities at boundaries between systems. This indicates that there is a case for the rail industry to adopt common security standards and practices as outlined, or referred to in this document and to be developed.

The impacts

1.20 There is potential for cyber attacks to cause damage and loss to rail networks. Successful cyber attacks could result in:

- threats to safety
- disruption to the rail network or services operating on it
- economic loss to rail operators, suppliers or the wider UK economy
- reputational damage to rail companies or the UK economy
- loss of commercial or sensitive information from the rail industry or suppliers
- criminal damage

1.21 There may also be potential to cause death and injury to those working on, or using the rail networks.

Resilience

Cyber systems and procedures adopted on the GB rail network should be designed, operated and maintained by the railway industry as a whole, to provide resilience against malicious attack.

Measures should be designed to limit the likelihood and impact of both deliberate and non-deliberate attacks in the first instance. They should also mitigate against the consequences of a successful attack.

The rail industry is best placed to implement cyber security resilience measures itself, with support from government.

1.22 While the main focus of this guidance is on deliberate attack, measures also need to consider:

- Non-deliberate attack through unintended infection with malicious software
- Attack caused by the use of online hacking tools
- Attack caused by hacking and unauthorised interrogation of systems
- Non-deliberate security breach through negligence or lack of knowledge

1.23 Cyber security measures and procedures considered appropriate in this guidance are those that focus primarily on terrorists, hackers, hacktivists and cyber criminals, and deliver value for money. This must be in keeping with a business case derived from robust Cost-Benefit Analysis (CBA) based on the ALARP principle, where likely benefits are considered to outweigh costs, while maintaining efficient and effective service. Risk management should be based on the ALARP principle. Benefits should focus on improved resilience.

1.24 For the purposes of this guidance, resilience should be considered to comprise:

- Reduction on the likelihood of attack, through good multi-layered design (defence in depth) and robust operational and maintenance procedures, with consideration given to the defence-in-depth principle, single points of failure and the role of non-cyber related fail safes
- Mitigation against disruption and failure once systems come under attack, through development, testing and maintenance of robust contingency plans
- Management and monitoring of the effectiveness of systems and procedures, to ensure optimum performance, and early warning of attack
- Contingency, recovery, and continued operation of the rail network
- The ability to facilitate investigation by police (and others) as far as practicable given the need to return the network to normal operation as a priority

2. Protecting infrastructure and rolling-stock systems

This guidance applies to electronic and software driven systems in use on rail (referred to as cyber systems in this guidance), including:

- new systems being introduced.
- legacy and current systems – defined respectively as technologically obsolete systems still in operation and current systems in operation mid-lifecycle.

This guidance applies to:

- operational (control and command systems) including signalling systems, The European Rail Traffic Management System (ERTMS), on-train systems and maintenance systems.
- business (corporate systems), with particular reference to their role as an interface to operational systems.
- shared systems (those co-owned by other organisations).

While operational systems and business systems are separate systems, industry should strive to bring controls as close together as possible (taking into account what is feasible, proportionate and appropriate) The Purdue Enterprise Reference Architecture (PERA) model provides a reference model for understanding cyber systems at an enterprise level. (pera.net)

Operational systems are those systems which are directly responsible for the functioning of the railway network infrastructure and rolling-stock. Business (corporate systems) are those systems that support the running of businesses in the industry or provide direct passenger interface.

Risk assessment and management

All organisations managing security risks on behalf of rail industry staff and travelling public should have a formal and comprehensive risk management system in place. Specific areas to consider are:

- governance
- cyber security in rail systems
- legacy/current and whole life-cycle systems
- third party systems
- review and future proofing
- communication and co-operation
- interfaces
- personnel capability/training

Governance

2.1 The overall governance of risk management in an organisation lies with corporate management, who are responsible for setting the overall approach, risk appetite and responsibilities.

Cyber security in rail systems

2.2 Design for safety, and safety management, are well established practices within rail. Management of cyber systems may be approached in a similar way.

2.3 Although safety measures may prove to be some protection against cyber threat, it is unlikely that existing safety measures can fully mitigate attack all types of attack.

Legacy/current and whole life-cycle systems

2.4 Risk assessments for new systems need to encompass all stages of their life cycles from design to decommissioning and disposal. Threats to security begin occurring from the design stage where vulnerabilities can arise from specifications that do not adequately take into account security good practice or produce inherent weaknesses. Systems already in place need to be assessed for vulnerabilities from their current state through to decommissioning and disposal.

2.5 Cyber security measures for legacy systems should be considered in accordance with how attractive a target they are, the likely impact and whether they are accessible to modern modes of attack e.g. hacking.

Third party systems

2.6 System functioning may include the transfer of data to and from, or through third party systems. It is unlikely that you will be able to have complete control over these systems' security provision. This is a risk which you should consider as part of your overall risk analysis.

See:

- Process Control and SCADA Security Guide 5 - Manage Third Party Risk (cpni.gov.uk)

Review and future proofing

2.7 Risks change over time. Consequently, risks must be periodically reassessed. Effective risk management systems contain periodic review points. Threats and vulnerabilities are reviewed at these points and where necessary action is mandated, or designated responses changed. Risk management systems should also allow for unscheduled reassessment in response to rapidly emerging threats or unexpected events.

2.8 Risk assessment should constitute an integral part of future proofing work – considering effective responses to future needs, requirements and challenges. IS1 Risk Assessment, and ISO 27000 outline standards and risk assessment methodology. These should be used in conjunction with other Centre for the Protection of National Infrastructure (CPNI) guidance, indicated below.

See:

- IS1 Risk Assessment (cesg.gov.uk)
- ISO 27000 (27000.org)
- Process Control and SCADA Security - General Guidance (cpni.gov.uk)
- Good Practice Guidelines - Process Control and SCADA Security (cpni.gov.uk)
- Process Control and SCADA Security Guide 1 - Understand the Business Risk (cpni.gov.uk)
- Process Control and SCADA Security Guide 2 - Implement Security Architecture (cpni.go.uk)
- Process Control and SCADA Security Guide 6 – Engage Projects (cpni.gov.uk)

Communication and cooperation

2.9 We strongly encourage communication and cooperation on cyber security between different organisations. We consider it mutually beneficial. It aids early warning, advice and good practice. We recommend, as a specific action, that your organisation joins the CISP. (www.cert.gov.uk/cisp)

Interfaces

2.10 You should put security measures in place at interfaces between systems inside organisations and between different organisations. These form part of system boundaries, and need protection. Trust cannot be assumed.

Principles for effective cyber security

- **'If it is not secure, it is unlikely to be safe'**: Claims about safety must be informed by security considerations.
- **proportionate response**: Security measures should be proportionate to the threat.
- **goal-based security**: As a general principle, DfT favours goal-based security. This means that a security level is set that the industry is expected to comply with.
- **designed-in security**: You should consider cyber security from concept development onwards.
- **Saltzer and Schroeder's design principles**: A set of 8 principles for designing secure systems

'If it is not secure, it is unlikely to be safe'

2.11 Claims about safety must be informed by security considerations. Security and safety are different but interrelated concepts. Security is related to deliberate and non-deliberate malicious acts. Safety is related to accidents, including those caused by lack of competence or negligence. If systems are unsecured, this leaves them open to malicious acts or non-deliberate compromise. Malicious acts in themselves may trigger safety events, including accidents. Failure to make systems secure might contravene regulatory safety requirements.

Proportionate response

2.12 Security measures should be proportionate to the threat. Security is an integral part of the broader running of any transport network. Security measures must be considered against the overall purpose of running the network efficiently and effectively for the travelling public and balanced accordingly. They must also be reasonable, when considered against the current and estimated future threat.

Goal-based security

2.13 As a general principle, DfT favours goal-based or outcome focussed security. We expect that organisations adopt methods for which there is a sound business case, and which do not contradict other principles listed here (e.g. proportionate response). In some cases there may be a compelling case to guide industry towards a certain method. Future detailed operational guidance will set out standards for cyber security.

Designed-in security

2.14 With new systems, you should consider cyber security from concept development onwards. It should not be considered as an addition or 'bolt-on' after concept and design stages. You should consider security to be a fundamental and integral part of any system.

Saltzer and Schroeder's design principles

2.15 A set of 8 principles for designing secure systems.

- **economy of mechanism**: keep the design as simple as possible
- **fail-safe defaults**: base access decisions on permission rather than exclusion
- **complete mediation**: every access to every object must be checked for authority
- **open design**: the design should not be secret
- **separation of privilege**: two keys are better than one
- **least privilege**: every program and every user of the system should operate using the least set of privileges necessary
- **least common mechanism**: minimise the amount of mechanism common to more than one user and depended on by all
- **psychological acceptability**: design for ease of use

Concepts for effective cyber security

Cyber security should be considered as one part of your general security package.

- **Protect**: Installing specific protection measures to prevent and discourage cyber attacks against the process control systems
- **Detect**: Establishing mechanisms for rapidly identifying actual or suspected cyber attacks
- **Respond**: Undertaking appropriate action in response to confirmed security incidents against cyber systems

Holistic security

- You should consider cyber security as an integral part of your general security package. It is interrelated with physical and personal security and not a 'stand-alone' concept.

Defence in depth

- Where a single measure has been deployed to protect a system, there is a risk that if a weakness in that measure is identified and exploited there is effectively no protection provided.

Protect, detect, respond

- Constructing a security framework for any system is not just a matter of deploying protection measures. It is important to be able to detect possible attacks and respond in an appropriate manner in order to minimise the impacts.

Technical, procedural and managerial protection measures

- When implementing security there is a natural tendency to focus the majority of effort on the technological elements. Although important, technology is insufficient on its own to provide robust protection. It is essential that people operate best practice.

Regulatory issues

- Security should be taken into consideration in safety cases.

Training

- Staff who will have contact with systems must be appropriately trained in complying with good security principles.

Defence in depth[1]

2.16 Where a single measure has been deployed to protect a system, there is a risk that if a weakness in that measure is identified and exploited there is effectively no protection provided. No single security measure itself is fool proof as vulnerabilities and weaknesses could be identified at any point in time. In order to reduce these risks, you should install multiple protection measures in series to avoid single points of failure. In order to safeguard the process control system from cyber attacks (e.g. hackers, worms and viruses), it may be insufficient to rely on a single firewall, designed to protect the corporate IT network. You should install a dedicated process security control, in addition to the corporate firewall. You should also deploy other protection measures such as anti-virus software and intrusion detection. Such a multi-layer security model is referred to as defence in depth. This approach is considerably more effective.

Protect, detect, respond

2.17 Constructing a security framework for any system is not just a matter of deploying protection measures. It is important to be able to detect possible attacks and respond in an appropriate manner in order to minimise the impacts.

- **Protect**: Installing specific protection measures to prevent and discourage cyber attack against end-points within or connected to cyber systems
- **Detect**: Establishing mechanisms for rapidly identifying actual or suspected cyber attacks and alerting
- **Respond**: Undertaking appropriate action in response to confirmed security incidents against the cyber systems

Technical, procedural and managerial protection measures

2.18 When implementing security there is a natural tendency to focus the majority of effort on the technological elements. Although important, technology is insufficient on its own to provide robust protection.

2.19 For example, when implementing a firewall, you must install and configure it correctly. However, you must also give consideration to associated procedural and managerial requirements:

- Procedural requirements may include change control and firewall monitoring
- Managerial requirements may include assurance of firewall installation and update, standards and training
- Updating Anti-Virus (AV) software.

[1] The Defence in depth principle is sometimes informally known as the ‘onion skin’.

See:

- Firewall Deployment for SCADA and Process Control Networks (cpni.gov.uk)

2.20 It is essential that people operate best practice. Your managerial practices should ensure that staff are aware of their roles and execute them effectively. It is also important to establish compliance activity (e.g. checking AV software is updated on laptops and USB ports are shut down).

Regulatory issues

2.21 Security should be taken into consideration in safety cases – you should ensure that the dossier of evidence that supports a system's compliance with safety regulation includes provision for cyber security. Ideally, the case will not require constant updating to take account of incremental changes to cyber security measures (e.g. routine updates to firewalls).

2.22 You should consider that systems with safety functions may be unsafe, if security has not been taken into account. Non-compliance may be addressed by the Office of Rail Regulation (ORR) in their capacity as safety regulator. You should put monitoring systems in place to ensure that you are able to detect malfunctions and suspicious activity. You should report this in line with requirements in Section 3: Handling Threats and Incidents – Immediate Action by Industry (para 3.9).

See:

- 10 Steps to Cyber Security (cpni.gov.uk)

Industry training

2.23 Training is an integral part of ensuring competence and capability to install and maintain secure systems throughout their entire lifecycle. You should ensure that all staff who will have contact with systems are appropriately trained and receive ongoing awareness training.

2.24 This should include, dependent on the level and scope of knowledge required:

- awareness of cyber security
- understanding what the problems are
- understanding why we need to consider security as well as safety
- understanding why security of control systems is different from security of IT systems
- the need to consider the whole life-cycle - not just deployment, also operation and maintenance
- the ongoing requirement for penetration testing[2]
- minimising impact on the safety case
- comparison with other sectors
- vulnerability management (including patching, Operating System (OS), firmware and application code)
- the importance of testing of equipment from manufacturer before it gets installed (AV) check, system change issues, system/network boundary awareness)

[2] Authorised attempts to breach the security defences of a system to ascertain their effectiveness.

See:

- Process control and SCADA security guide 4 - Improve Awareness and Skills (cpni.gov.uk)

2.25 The Government's National Technical Authority for Information Assurance, CESG, has established CESG Certified Training (CCT) to help equip people with the skills needed to effectively manage the security risks and threats to business from cyber-attack. GCHQ certifies a number of Master's degrees in cyber security with the aim to identify and recognise the very best cyber security education in the UK.

See:

- CESG Certified Training (apmg-cyber.com)
- CESG Master's degrees (cesg.gov.uk)

2.26 Research on UK Cyber Security Standards (bis.gov.uk) conducted by BIS in 2014 concluded that Certified Information Systems Security Professional (CISSP) (isc2.org) is the most desirable qualification for cyber security. The Certified Security Software Lifecycle Professional (CSSLP) handbook also provides comprehensive guidance for software developers on how to develop security software. Common body of knowledge handbooks are available from The Information Systems Audit and Control Association (ISACA). (isaca.org.uk)

Designing in security

Security requirements for systems are more effective when considered as an integral part of those systems. You should design in security requirements from the start of the design process. With this in mind, good practice indicates that you should stipulate compliance by procurers, with security standards being developed, as part of the product specification.

In addition, you should put mechanisms in place to ensure that security systems are upgraded, updated and maintained for the duration of their life cycles. You should also ensure that systems are disposed of securely to ensure that data is effectively deleted.

See:

- Cyber Security Procurement Language for Control Systems (ics-cert.us-cert.gov)

You should consider five areas when looking to procure a new system or when upgrading any part of a current system:

- **design**: systems using modern technologies, including Transmission Control Protocol//Internet Protocol (TCP/IP), MODBUS (serial communications protocol) and other standardised protocols, should be designed with security in mind as an integral part of the system
- **development**: recognised secure software development standards exist that should be used when developing software to be used within any environment.

- **installation**: installation of the new or upgraded system should not compromise the security that has already been put in place. It should not increase the attack surface that could be exploited by an attacker.
- **maintenance**: you should maintain systems throughout their life cycles to ensure optimum functioning.
- **decommissioning and disposal**: you should decommission systems and dispose of them securely to prevent the possibility of hostile 3rd parties acquiring your data.
- **independent validation**: ensuring security implementations and security products have a level of assurance that has been tested

Design

2.27 Systems using modern technologies, including TCP/IP, MODBUS and other standardised protocols, should be designed with security in mind as an integral part of the system. You should consider security in every aspect of the system, from specification of requirements and, software and application design, to the architecture of any communications system.

2.28 You should put protective measures in place on communications systems, train control and signalling interfaces, power and traction control signalling and business/corporate systems, to identify and bar unauthorised transmissions, and limit the data travelling over links other than those which are specifically intended for transmission. Protective measures should be put in place to bar unauthorised access. You should monitor and update them regularly as part of Standard Operating Procedure (SOP). Systems should also be monitored and underlying architecture analysed for failure and abnormal performance.

2.29 Wherever practical you should consider a direct acting “hard wired” safety system in the system architecture so that there is no dependence on software for safety features. **This is currently an absolute requirement for rolling stock emergency brake requests.**

2.30 You should give consideration to how much system design detail should be made publicly available, particularly where there are direct implications for cyber security.

See:

- National Institute of Standards and Technology (NIST) (nist.gov.uk)
- Industrial Control Standards (ul.com)
- Securing the Move to IP Based SCADA/PLC Networks (cpni.gov.uk)
- Cyber Security Assessment of Industrial Control Systems (cpni.gov.uk)
- BSIMM/SafeCode Guidance and Recommendations (www.safecode.org)

Development

2.31 Recognised secure software development standards exist that should be used when developing software in any environment. These include Microsoft Security Development Lifecycle, SAFECode guidance, Building Security in Maturity Model (BSIMM) best practice, and Open Web Application Security Project (OWASP)

Top 10. Whichever development approach is chosen, it is important you ensure that the following key areas are included:

- threat modelling / architectural risk analysis
- attack surface reduction[3]
- 'fuzz' testing[4]
- static analysis[5]

See:

- Building Security In Maturity Model (BSIMM) (bismm.com)
- Microsoft Security Development Lifecycle (microsoft.com)
- Fundamental Practices for Security Software Development (safecode.org)
- Open Web Application Security Project (OWASP) (owasp.org)

2.32 You should also consider effective quality assurance techniques to ensure that the development of the software is following the secure development process chosen. The key goal of secure development is to reduce the surface for attack. PAS 754 is a recognised standard to support quality assurance.

2.33 You should specify cyber security requirements in contract requirements, and ask for evidence of security features and vulnerabilities in the procured products to clearly define the risk profile of the systems on an individual basis. You should also assert the right to audit the development environment and the security of the development, testing, chain of custody and shipping process. Your will need to ensure that procurement staff are sufficiently skilled in cyber security, in order to be able to articulate requirements correctly. Ideally, you should reference a risk assessment methodology and:

See:

- ISO27001 (iso.org)
- ISO27005 (iso.org)

Installation

2.34 Installation of the new or upgraded system should not compromise the security that has already been put in place. It should not increase the attack surface that could be exploited by an attacker. You must:

- set system boundaries. Boundaries exist at interfaces with other organisations and within specific organisations, between different areas of function. Where possible there should be an 'air gap' or clear separation between systems
- complete a risk analysis
- put mitigations in place that allows the equipment to be reset or restarted.

[3] The 'attack surface' is the set of interfaces that are exposed to unauthorised users
[4] 'Fuzz testing' is the process of bombarding systems with known code to find weaknesses.
[5] 'static analysis' is simplified analysis wherein the effect of an immediate change to a system is calculated without respect to the longer term response of the system to that change.

2.35 You should scan all new equipment and software for malware. We recommend that this function is performed as a standard part of pre-installation bench testing.

2.36 You should consider the possibility that new equipment and software might contain functionality capable of compromising cyber security. You should require disclosure by the supplier of any functionality in the equipment or software:

- that allows internet access
- that allows the supplier remote access to the equipment or software, post-installation
- that allows the supplier to transmit data to the equipment
- that allows the supplier to retrieve data from the equipment remotely
- that allows the equipment to send data to the supplier
- that allows the supplier to re-programme systems

2.37 You will need to decide on a risk basis, whether such functions should be enabled. If they are to be enabled, you should guarantee compliance with incoming cyber security standards derived from this guidance under contract.

2.38 You should specify the functionality that should be enabled or disabled in all new equipment and software in contracts with suppliers.

2.39 You should also consider the sources of equipment and software. Some suppliers have been implicated in facilitating hostile state activity (industrial espionage) through the deliberate supply of infected equipment and software. Some suppliers do not adequately secure their products, allowing non-deliberate infection with malware. You should seek advice from CPNI on mitigating the threats posed by suppliers.

2.40 As a general principle the onus should be put on the supplier to adhere to proscribed security standards or be in breach of contract. However, given the complexity of supply chains, security cannot be assumed. New systems should be tested on receipt and before commissioning for pre-existing malware.

2.41 Security should be a key part of your ongoing system design. No changes should be made without risk analysis and understanding of the impact that they might create from a security angle.

2.42 Points to consider are:

- changes in threat environment
- ensuring there is a response plan in place
- running exercises to test incident response
- resilience of systems
- networks
- architectures and physical locations/infrastructure.

2.43 New systems should contain:

- authentication between devices
- protection against unauthorised access
- malware protection

2.44 You will need to design systems to ensure that they are robust. Penetration testing is a well established tool for testing the effectiveness of security systems. 'White hat', or 'friendly' hackers can be employed to do this.

Maintenance

2.45 You should maintain systems throughout their life cycles to ensure optimum functioning. You should keep abreast of new developments in malware and other threats, through engagement with organisations such as CPNI and the CISP. You should test systems on a regular basis for new vulnerabilities or areas that may have become newly vulnerable as a result of a new threat. Part of your planned maintenance schedule should be updating and patching of security software. You should also update and patch systems as and when required.

2.46 You should ensure that systems are analysed on a regular basis to identify abnormal functioning or indications of suspicious behaviour.

See:

- www.cpni.gov.uk
- www.cert.gov.uk/cisp

Decommissioning and disposal

2.47 You should decommission systems and dispose of them securely to limit the possibility of hostile third parties acquiring your data. Threats may arise from:

- accidental loss;
- emergency abandonment (individual, vehicle or building);
- espionage (commercial or state sponsored);
- hijack or vehicle theft (from site or during transportation);
- insider attack (e.g. disgruntled employees or investigative journalists);
- theft (from site, vehicle, storage or destruction facility).

See:

- Secure Destruction of Sensitive Information (cpni.gov)

Protecting against attacks on new and current systems

Critical controls for effective cyber defence

- **The Critical Security Controls for cyber defence are a baseline of high-priority information security measures and controls that can be applied across an organisation in order to improve its cyber defence.**

See:

- Critical Security Controls Guidance (cpni.gov.uk)

General guidance applicable to all systems

- **Patching and updates**. You should identify and classify all cyber systems and components that are safety related and might require patching or updates.

- **Train control and signalling**. You should physically or electronically separate on-train networks for passengers from networks used for train control and signalling, particularly where WiFi is used.
- **Physical and cyber attacks.** Cyber attacks and physical attacks are fundamentally different in their nature. However, they are related in that each can facilitate the other.
- **Cabling**. Cables into buildings and cabinets containing command and control infrastructure need particular protection from physical attacks that might facilitate cyber attacks.

Other issues to consider

- **Capability and competence**. It is important that organisations have the human resources to maintain cyber security.
- **International issues**. You should consider the implications of working with organisations from other countries. Cyber security standards in other countries may be different to those in the UK.

General guidance applicable to all systems

Patching and updates

2.48 You should identify and classify all cyber systems and components that are safety related and might require patching or updates. Some systems and equipment are classed as safety related and so are subject to a safety case. Patches or updates made to a safety related system might violate the safety case.

- all systems and equipment that are non-safety systems (or below Safety Integrity Level - SIL 1) should have anti-virus software fitted. For end-points that cannot run anti-virus or be regularly patched use alternatively methods to prevent known attacks against susceptible end-points.
- all systems and equipment that are non-safety systems (or below SIL 1) should be updated and patched.
- all systems and equipment that are SIL 1 to SIL 2 should be updated and patched where this does not violate the safety case.
- you should consider whether systems and equipment at SIL 3 to SIL 4 can be updated and patched without violating the safety case. Where the safety case will not be violated, updating and patching should be undertaken.
- you should design all future systems and equipment at SIL 3 to SIL 4 so that they can be patched without violating the safety case.
- you should analyse the network architecture and the systems segmented behind firewalls (which are maintained, updated and monitored) and any other protective mechanism, to restrict access.
- you should set up firewalls and switches in accordance with manufacturers' instructions, patch, maintain and monitor as a matter of normal standard operating procedure. Signals should ideally contain unidirectional gateways.

Train control and signalling interface

2.49 You should physically or electronically separate on-train networks for passengers from networks used for train control and railway signalling, particularly where Wi-Fi is used, i.e. there should be an 'air-gap' preventing direct passenger access to a train's control and command systems.

Physical and cyber attacks

2.50 Cyber attacks and physical attacks are fundamentally different in their nature. However, they are related in that each can facilitate the other. A physical intrusion could allow a cyber attacker into a restricted area to hack into a system. Conversely, a cyber attack could facilitate access to a restricted area by a physical attacker.

2.51 It is very important as a general principle that physical and cyber security regimes are integrated and so can function harmoniously.

See:

- Physical Protection of Cell Sites (cpni.gov.uk)

Cabling

2.52 Cables into buildings and cabinets containing command and control infrastructure need particular protection from physical attacks that might facilitate cyber attacks i.e. cutting fibre-optic or copper cables and linking them to hardware. You should provide physical security in accordance with CPNI guidance.

2.53 You should strictly control switching room access in accordance with CPNI physical security guidance.

See:

- CPNI Perimeters and Access Control Guidance (cpni.gov.uk)

Other issues to consider

Capability and competence

2.54 It is important that organisations have the human resources to maintain cyber security. It is equally important to ensure that employees are suitably trained and that their knowledge is regularly updated to keep up with rapidly changing risks.

International issues

2.55 The internet is inherently global – transcending national boundaries. Your organisation may operate on an international basis through procurement, service delivery or web hosting. You should consider the implications of working with organisations from other countries throughout the supply chain. Cyber security standards in other countries may not be equivalent to those in the UK. Furthermore, some countries may harbour malicious intent towards the UK and its industries. Advice is available from CPNI (cpni.gov.uk)

3. Handling threats and incidents

The UK Government has a National Cyber Security Incident Management Policy (NCSIMP) owned by the Cabinet Office. This informs a Cyber Incident Co-Ordination Plan (CICP). This is owned by CERT-UK.

The DfT has an incident response framework for internal use. This will be invoked dependent on the level of incident and its effect.

You should have in place your own emergency response/contingency plans. You should invoke them in line with internal policy, informed by this guidance.

The relationship between these documents is displayed in Fig .1

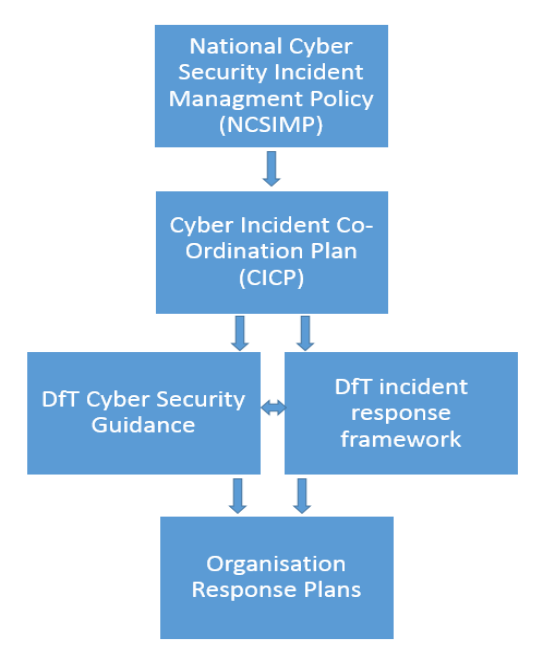

Fig. 1 - The relationship between governmental and organisational documents governing handling of cyber attacks.

Where the CICP and incident response framework have been invoked, you should ensure that your actions are in step with both. You should ensure that you comply with requests and instructions given by government and/or orders given by the police. Where you are unable to comply, you should make this known immediately to the originator.

See:

- Process Control and SCADA Security guide 3 – Establish Response Capabilities (cpni.gov.uk)

A rise in threat level or unexpected attack

Action when intelligence indicates a rise in threat

Action by government:

DfT will issue a message to industry representatives informing them of the nature of the threat, the likely impact and any change to threat levels.

Immediate action by industry:

You should refer to CERT-UK for first response

Action when an attack occurs unexpectedly

The action required is dependent on the severity of the attack that has taken place. There is a 5-level system (0-3) which indicates correct responses. Level 0 is divided into 2 sub-levels.

- Level 0: Steady State
- Level 0: Exceptional Occurrence
- Level 1: Significant Emergency
- Level 2: Serious Emergency
- Level 3: Catastrophic Emergency

National Incidents

3.1 National incidents are declared by CERT-UK when an incident cannot be managed through normal arrangements and the assistance of other stakeholders and DfT as Lead Government Department is necessary.

3.2 Some incidents that are in the process of being managed may only have a cyber element identified at a later stage.

3.3 A national incident can be escalated and de-escalated without going through each level of emergency.

3.4 **Level 0: Steady State** - normal operational conditions where there are constantly occurring cyber security events of varied severity, with responsibility for responding and resolving them remaining with the organisations affected. However, any unusual activity should be reported to CERT-UK.

3.5 **Level 0: Exceptional Occurrence** - The category of Steady State occurrences:

- which will generate sufficient public and/or ministerial interest.
- where CERT-UK coordination will **add value to** an incident or number of linked incidents.

3.6 **Level 1: Significant Emergency - Requires central Government support by the Lead Government Department**. Examples of this level of incident include those which threaten or have caused:

- degradation on networks supporting the operation of the critical national infrastructure, or on Government networks which are linked to online service delivery;

- widespread theft of intellectual property against the UK which may result in major financial loss or loss of technical advantage;
- media reporting which undermines public trust and confidence in online services and the Government cyber response.

3.7 **Level 2: Serious Emergency** - Requires **sustained central Government co-ordination** from a number of departments and agencies. The central Government response to such an emergency would be **coordinated from COBR**. Examples of this level of incident will include those which threaten or have:

- significant impact on the critical national infrastructure or Government systems providing critical services e.g. disruption of food delivery, water or power supply, or national communications.
- significant reputational impact on the UK – often linked to events which place the UK on the international stage, e.g. the Olympics.

3.8 **Level 3 Catastrophic Emergency** - Requires **immediate central Government direction** from a number of departments and agencies. The central Government response to such an emergency would be **coordinated from the Cabinet Office Briefing Rooms (COBR)**. Examples of this level of incident will include those which threaten or have already resulted in:

- simultaneous loss of a number of critical services (e.g. power, water and telecommunications) affecting a single region.
- loss of a single essential service to the whole of the UK over a sustained period.

Immediate action by industry

3.9 A cyber attack may not be immediately identifiable as such. It may initially appear to be a system failure or non-deliberate act. The consideration of malicious activity should be part of the algorithm used to govern the diagnostic process. This should be placed, in order of execution, after more likely non-malicious causes, and considered when these causes can be reasonably ruled out in accordance with established procedure.

3.10 You should look for one or more of the following:

- coincidence with another security breach, perhaps physical
- records indicating the connection of an unauthorised media or data storage device
- instructions issued from unexpected sources internally
- instructions issued from unknown or suspicious sources externally
- abnormal, illogical or otherwise obviously suspicious instructions being issued from any source
- recently imported data
- recent activation of unknown software or script
- unauthorised disabling of firewalls, or security software
- unauthorised deletion or alteration of data
- drops in light levels in fibre-optic cables

3.11 The threshold at which you should report an incident is set at the point where an incident has reached, or you have reason to believe it will reach, Level 0: Exceptional Occurrence. You should send your report to the CERT-UK and the British Transport Police (BTP). This does not preclude you from consulting the CERT-UK regarding steady state activity (for situational awareness). Where an attack has had implications for safety or has caused significant disruption to services, you should also inform DfT Threats Office or the DfT Duty Office (out of hours) and the ORR in accordance with contact details supplied.

Communication to the public

3.12 It is important to balance the public 'need to know' with the need to maintain public order. In common with all other emergency situations, it is very important to avoid causing panic. This may lead to additional safety incidents and reputational damage.

3.13 **The safety of people and where appropriate, their safe evacuation, is the highest priority**. You should focus your communications to the public on ensuring their safety. Focus on the impact and not the causes of the emergency, unless disclosure is integral to maximising safety efforts. The source of an attack may be a terrorist group. This may actually be a relatively minor event where there is no significant threat to the safety of staff and the travelling public. Terrorism and terrorism-related words are emotive. They are associated with death and serious injury. Use of these words would likely cause panic and a disproportionate media response, despite the actual impact. During an Exceptional Occurrence, all media lines should be agreed with these organisations prior to release, to ensure a consistent message. During a national incident, media lines should be consistent with the lines agreed by the incident co-ordination groups set out in the NCSIMP.

See:

- ATOC Guidance Note – Major Incidents – Preparation of Aide Mémoires for Senior Managers (atoc.org)
- Supporting Survivors – a guide outlining help for helping people in a crisis (atoc.org)

3.14 There is a high risk of reputational damage to organisations from a successful cyber attack. We recommend that public disclosure of the causes of an event should only be made known when there is compelling evidence to demonstrate a malicious event. You should discuss disclosure with DfT, BTP and CERT-UK prior to release. In the event of such an attack, disclosure might impact on investigations. All media lines should be agreed with these organisations prior to release, to ensure a consistent message.

Contingency in the event of a cyber attack

Immediate actions

The safety of people is the highest priority and the first to be considered. In the event of any cyber attack, you must ensure that equipment is made safe and access paths made clear, to enable the emergency services to access injured people, where they are required. **This overrides all other considerations**.

Continued operations

When systems and equipment have been made safe, there are further priorities. These are in order of importance:

- starting limited, degraded operation where the risk to safety is acceptable, in accordance with usual practice.
- returning the network to its normal state of functioning.
- taking any remedial action where the point of breach has been identified.
- identifying, isolating and preserving evidence for forensic analysis.
- internal investigation into how systems were breached (this must not interfere with any official investigation).
- remedial action to prevent further breaches.

Criminal Investigation by police

In the event of a cyber attack, it is likely that a crime has taken place.

As a general principle, the BTP accept that restarting services may take precedence over the preservation of evidence in the event of cyber attacks. However, subject to this, preservation of evidence is still a priority as outlined above.

3.15 Where the emergency services are not required, the safety of people still remains the first priority. Affected systems and equipment must be put into a safe state to prevent harm or damage occurring after the initial attack has taken place.

3.16 Where a hacker or piece of malware has gained unauthorised access, you must ensure the point of entry and other potential points of entry have been secured. In the event of an attack using malware, you must ensure that the malware has been completely removed from the infected system(s).

3.17 You should give consideration to the preservation of evidence where this will not have a critical impact on restarting services. Where multiple systems exist, one system could be preserved in its degraded state for forensic purposes.

Priorities in the event of an attack

The safety of people is the highest priority. This overrides all other considerations. When systems and equipment have been made safe, the next priority is starting limited, degraded operation where the risk to safety is acceptable.

Clear up and recovery

Both the CICP and the DfT incident response framework run from the beginning of an emergency event to the point where recovery begins and businesses head towards their usual steady states of operation.

Coordination: Where the CICP and the DfT incident response framework have been invoked, HM Government will communicate details to industry and continue to coordinate recovery efforts.

Action by industry: Where the CICP and DfT incident response framework have been invoked, you should carry out procedures in accordance with your internal emergency response and contingency plans, provided that their provisions do not clash with the CICP. The CICP should take precedence over internal plans.

Services cannot recommence unless the risk to human safety is considered acceptable, as in any other emergency situation. Dependent on the severity of the event, this decision may be made by the Cabinet Office Briefing Rooms (COBR) Committee.

You should take the opportunity to learn from what went well and what did not work so well.

3.18 Where the CICP and the DfT incident response framework have not been invoked (i.e. at level 0 steady state, and possibly at Level 0 Exceptional Occurrence), you should coordinate your own response in accordance with your own emergency response and contingency plans.

3.19 Where an attack has taken place, you should consider the risk from further attack, and specifically the potential threat to human safety that this might cause. You should take advice from CERT-UK on the likelihood of further attacks taking place.

Lessons learned and continual improvement

3.20 Cyber attacks and their consequences are highly undesirable, resource intensive and may risk the safety of passengers and staff. However, they also provide an opportunity to learn lessons and improve future performance in crisis management and disaster recovery. These lessons can be used to update your emergency response and contingency plans. Learning lessons and continual improvement will enhance responses to emergency-related strategic risks. We recommend that you produce a lessons learnt report.

3.21 Exercises are a good way of testing internal systems and responses. We recommend that you put in place a regular exercising programme for cyber related incidents.

Annex A: Links

Information	Link
10 Steps to Cyber Security	cpni.gov.uk
20 Critical Controls for Cyber Defence	cpni.gov.uk
ATOC Guidance Note – Major Incidents – Preparation of Aide Mémoires for Senior Managers	atoc.org
Building Security In Maturity Model (BSIMM)	bismm.com
Centre for the Protection of National Infrastructure (CPNI)	cpni.gov.uk
Certified Information Systems Security Professional (CISSP)	isc2.org
Certified Security Software Lifecycle Professional (CSSLP) handbook	isc2.org
CERT-UK	cert.gov.uk
CESG Certified Training	apmg-cyber.com
CESG Master's degrees	cesg.gov.uk
Configuring and Managing Remote Access for Industrial Control Systems	cpni.gov.uk
CPNI Perimeters and Access Control Guidance	cpni.gov.uk
Cyber Essentials	gov.uk
Cyber Security Assessment of Industrial Control Systems	cpni.gov.uk
Cyber Security Information Sharing Partnership (CISP)	cert.gov.uk/cisp
Cyber Security Procurement Language for Control Systems	ics-cert.us-cert.gov
Firewall Deployment for SCADA and Process Control Networks	cpni.gov.uk
Fundamental Practices for Security Software Development	safecode.org
Good Practice Guidelines - Process Control and SCADA Security	cpni.gov.uk
Guide to Industrial Control Systems Security	csrc.nist.gov
Industrial Control Standards	ul.com

Information	Link
IS1 Risk Assessment	cesg.gov.uk
ISA62443	isa99.isa.org
ISO 27000	27000.org
ISO27001	iso.org
ISO27005	iso.org
Microsoft Security Development Lifecycle	microsoft.com
National Institute of Standards & Technology (NIST) cyber security framework	nist.gov.uk
National Institute of Standards and Technology (NIST)	nist.gov.uk
Open Web Application Security Project (OWASP)	owasp.org
Physical Protection of Cell Sites	cpni.gov.uk
Process Control and SCADA Security - General Guidance	cpni.gov.uk
Process Control and SCADA Security Guide 1 - Understand the Business Risk	cpni.gov.uk
Process Control and SCADA Security Guide 2 - Implement Security Architecture	cpni.gov.uk
Process Control and SCADA Security guide 3 – Establish Response Capabilities	cpni.gov.uk
Process control and SCADA security guide 4 - Improve Awareness and Skills	cpni.gov.uk
Process Control and SCADA Security Guide 5 - Manage Third Party Risk	cpni.gov.uk
Process Control and SCADA Security Guide 6 – Engage Projects	cpni.gov.uk
Process Control and SCADA Security Guide 7 - Establish Ongoing Governance	cpni.gov.uk
Purdue Enterprise Reference Architecture (PERA)	pera.net
Remote Access for ICS	cpni.gov.uk
Research on UK Cyber Security Standards	bis.gov.uk
SafeCode	safecode.org
Secure Destruction of Sensitive Information	cpni.gov.uk
Securing the Move to IP Based SCADA/PLC Networks	cpni.gov.uk

Information	Link
Supporting Survivors – a guide outlining help for helping people in a crisis	atoc.org
The HM Government Security Policy Framework.	gov.uk
The Information Systems Audit and Control Association (ISACA)	isaca.org.uk

Annex B: Glossary of Terms

Note: Some definitions used in this glossary are given as they specifically apply to cyber security in this guidance document and should not be considered absolute definitions.

TERM	DEFINITION
As Low As Reasonably Practicable (ALARP)	The point at which reducing the risk further in terms of the trouble, time and cost involved would be grossly disproportionate to the benefit gained.
Attack surface	The set of interfaces that are exposed to unauthorised users
Best Practice	Activities towards a specific outcome, or specific outcomes, considered to be optimum, or most efficient and effective.
BSIMM	Building Security in Maturity Model. A system designed to help your understanding, measuring and planning of a software security initiative.
Centre for the Protection of National Infrastructure (CPNI)	The UK government authority charged with protecting national security by providing protective security advice on physical, personnel and cyber security.
Commercial Off The Shelf (COTS)	Widely used and non-bespoke.
Computer Emergency Response Team for the UK (CERT-UK)	An organisation of the UK Government charged with monitoring, response and coordination for cyber security at a national level.
Cost Benefit Analysis	An assessment of likely positive outcomes of any policy, procurement or procedure, against the relative costs, to ascertain whether or not those outcomes are worth the cost incurred (cost effective).
Cyber Security Information Sharing Partnership (CISP)	An initiative hosted by CERT-UK to bring together industry to share good practice and information on incidents in a confidential environment.

Defence in Depth	The security principle stating that the strength of a security system is grounded in its composition from multiple protection measures (aka 'onion skin security')
European Rail Traffic Management System (ERTMS)	A rail traffic management system designed to replace existing national control and command systems in European Union Member States. It comprises: The European Train Control System (ETCS). Global System for Mobile Communications – Railway (GSM-R)
European Train Control System (ETCS)	A signalling, control and automatic train protection designed to replace the existing national systems.
Fuzz Testing	The process of bombarding systems with known code to find weaknesses.
Global System for Mobile Communications – Railway (GSM-R)	A radio system for providing voice and data communication between the track and the train, based on standard GSM using frequencies specifically reserved for rail application with certain specific and advanced functions.
Holistic Security	The theory and practice of security management which considers all aspects of security together as an integrated, interdependent whole.
Hostile Actor	Any person or organisation or nation who acts in a malicious way towards a system, or systems, being protected.
Insider threat	A threat posed by a hostile actor, or hostile actors, working inside an organisation.
Impact	The sum total of the damage resulting from a successful attack.
Industrial Control System	Any system designed to operate and manage any aspect of an industrial process.
National Institute of Standards and Technology (NIST)	A non-regulatory federal agency within the United States Department of Commerce designed to promote US innovation and industrial competitiveness by advancing measurement science, standards and technology.
Network Boundary	The outer limit of a single network that can be considered as an interrelated whole for operational, control and governance purposes.
Resilience	The ability to withstand and subsequently recover from attack.

Risk	Risk is defined by the Office of Government Commerce (OGC) as: 'an uncertain event of set of events that, should it occur, will have an effect on the achievement of objectives. A risk is measured by the combination of the probability of a perceived threat of opportunity occurring and the magnitude of its impact on objectives.' With security risks specifically in mind, likelihoods and impacts are primarily defined by the threats and vulnerabilities that exist. Note: Risks are usually perceived in negative terms. In fact, a risk may be negative or positive. In the latter case, opportunities replace threats.
Risk Management	Risk Management is defined by the OGC as: 'the systematic application of principles, an approach and process to the tasks of identifying and assessing risks, and then planning and implementing risk responses.'
OWASP	Open Web Application Security Project. This is a not-for-profit organisation providing practical, cost-effective information about application security.
Penetration Testing	Authorised attempts to breach the security defences of a system to ascertain their effectiveness.
SCADA	System Control and Data Acquisition. A system operating with coded signals over communication channels so as to provide control of remote equipment (using typically one communication channel per remote station).
Standard Operating Procedure (SOP)	The agreed and mandated way of operating a system or network under normal working conditions.
Threat	The danger posed by a hostile actor.
Vulnerability	A weakness in information systems, system procedures, controls, or implementations that can be exploited by a threat source.
'White Hat' hackers	'Friendly' hackers employed to test the effectiveness of security systems.

Annex C: Summary of proposed actions for industry

Assessment of Risks	Industry should assess the risks to the security of its systems on a regular and iterative basis.
Inform DfT and ORR	In the event of an attack, where the criteria outlined in section 3 are met, organisations that have been attacked should inform DfT and ORR.
Join CISP	Individual organisations should join CISP
Voluntary Security Standards	Industry to consider wording and content of Voluntary Security Standards with the RSSB.