CYBER SECURITY PRINCIPLES FOR THE WATER INDUSTRY

A report from the Water UK Cyber Security Good Practice Group

Water UK

Version 1 2017 (Final)

NOTE

This document is produced in response to a Defra document therefore covers English water companies. Water companies in Wales, Scotland and Northern Ireland may also find these principles and good practice useful but consideration will need to be given to the specific legislation in these devolved administrations.

Version Control

Version 1: 5 January 2016 – report approved by project board for internal circulation to water companies. Circulated to Water UK Council and technical networks.

Contents

Foreword

The UK Water Industry provides a unique challenge when it comes to implementing cyber security. The combination of critical national infrastructure, complex investment cycles and legacy hardware, alongside an evolving regulatory framework means that most companies are now juggling priorities to address the risks identified alongside other significant investments.

Threats from cyber-attack are increasing at the same time as legacy technology reaches its end-of-life, creating a pressure on companies to prioritise investment strategically. In addition, the technology landscape is changing and presents new challenges to traditional information technology and operational technology investment. Such changes must be managed and balanced against competing commercial and industrial challenges.

Additionally, water companies are organisations of varying sizes, structures, asset histories, and capabilities. Across the industry, this presents a challenge in developing a common approach to cyber security.

The Water UK Cyber Security Good Practice (CSGP) Group was formed in May 2016 to consider where industry good practice could be shared. In developing this good practice guide, we have taken the best of sector practice, developed ideas and approaches to managing security, and reviewed the plethora of existing standards. The standards and best practice guidelines outlined here do not represent a list of mandatory activities. However, the consensus is that they represent a resource to complement existing activities and help water companies prepare for cyber threats. The CSGP Group recognises there may be different ways of assessing risk and preparing water organisations. In undertaking this work we have prepared a list of tools that companies could use to their benefit.

The UK Water Industry is keen to work with the UK government and its partners, to demonstrate and develop our planning and investment programmes. Many companies have already taken steps to develop new governance frameworks, maturity models and policies in relation to cyber security.

We recognise that there is still some way to go to address and mitigate threats from cyber but affirm that this report is a step on that journey. As part of ongoing development, an electronic toolbox of resources and base materials will be made available to water companies in early 2017.

Phil Chatterton, Chair of Water UK Cyber Security Good Practice group
January 2017

Executive Summary

UK Government recognises that there is a credible threat to the nation's Critical National Infrastructure (CNI). Cyber-attack ranks with international terrorism, state-based threats and changes in established international order as one of the serious national security challenges facing the UK.

During 2015 and 2016, Defra assessed the water industry's maturity of cyber security preparation. They identified that improvements need to be made, which may require investment to improve the current low-to-medium maturity score.

The risks are very dynamic within cyber security, but at the time of writing, the biggest risks within the water industry are seen as:

- Accidental or deliberate misuse of information systems within a water company, (known as an insider threat);
- The growing industry move to integrate and join Information Technology (IT) and Operational Technology (OT) to benefit from cost efficiencies creating a different risk landscape that needs to be controlled;
- Phishing campaigns and other fraud-type activities.

Defra, as the lead government department for the water sector, together with the Centre for the Protection of National Infrastructure (CPNI), the National Cyber Security Centre (NCSC), Ofwat and the Drinking Water Inspectorate (DWI) are developing materials and strategies to help companies address these risks.

The water industry in the UK recognises the risks and the need to invest to improve systems and processes as well as developing practices by which to improve preparedness, share intelligence and adopt controls. It also recognises that the cyber threat is evolving and seeks to understand how the changing threat landscape can be identified and then mitigated or managed.

This document, produced by the Water UK Cyber Security Good Practice group (Appendix 1) in collaboration with Defra and the National Cyber Security Centre (NCSC), is provided to water companies as a helpful tool. This guidance identifies six core principles and provides recommended good practice for each principle. It references industry standards including NIST, ISO and CPNI advice and is supplemented with practices and examples of work which are being undertaken within the sector. This guide includes sample materials which could be used by companies to develop the sector's maturity.

The six principles and key recommendations are as follows:

Principle 1: To have robust and accountable cyber security governance

- Recommendation 1: Create strong governance structures that ensure cyber security is considered and managed, with ownership and accountability from the top of the company.
- Recommendation 2: Develop and maintain policy documents, standards and guidelines.

Principle 2: To manage cyber risk and compliance proactively

- Recommendation 3: Demonstrate that cyber risks are accommodated within the risk management system.
- Recommendation 4: Develop continuous improvement initiatives aimed at addressing threat, risk and readiness.

Principle 3: To ensure all our people are cyber aware with suitable training and communication

- Recommendation 5: Continue to increase awareness and cyber skills within their wider workforce.

Principle 4: To make best use of good threat intelligence

- Recommendation 6: Identify sources of good, reliable and credible intelligence.
- Recommendation 7: Encourage industry knowledge sharing and participation.

Principle 5: To improve incident response

- Recommendation 8: Ensure incident response and recovery plans are in place and tested.

Principle 6: To manage procurement, third parties and the wider supply chain proactively

- Recommendation 9: Understand the interactions with existing third party service providers and the reach within water company operations.
- Recommendation 10: Actively ensure third parties are aware of, and comply with, their obligations and the policies of cyber security within your organisation, from procurement to ongoing contract management.

1: Introduction

1.1 Background

The three aspects of protective security comprise physical, cyber and personnel. The amount of legislation and governance differs across the three dimensions.

Protective security is legislated in England and Wales by the Water Industry Act 1991, as amended. Physical security is addressed via the Security and Emergency Planning Directive (SEMD), originally published in 1998, and supplemented by numerous Advice Notes (ANs). Companies participate in an annual SEMD audit, generally lasting three days. In addition, the water industry via Water UK has developed sector-specific advice and good practice (SSAOA), which has been adopted by all companies.

As of December 2016, there is a single Advice Note for cyber security focussing on SCADA[1], requiring companies to participate in an annual self-assessment that is presented to Defra. It is expected that the NCSC will develop new tools and approaches to help companies manage cyber risks.

As yet, there is no sector-specific guidance for personnel security – a gap which has been recognised and will be a focus of the sector in during 2017.

In 2016, Defra produced the discussion paper *"Water sector cyber security 'guiding principles"*. The paper identified that Defra, in the spirit of working towards principles-based regulation, wishes to avoid taking a prescriptive approach to cyber security. Defra has indicated its intentions to move to a more proportionate approach to its guidance. Figure 1 has been reproduced with Defra's permission, but it should be noted that this is an indication of Defra's thinking at the time of writing, and not official public policy.

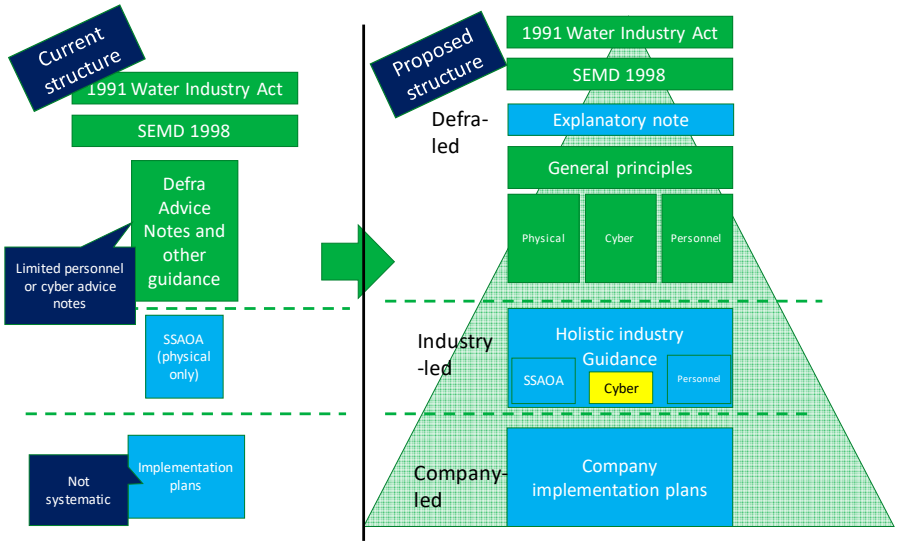

Figure 1: Defra's proposal to develop the existing protective security guidance suite for the water sector

[1] SCADA (supervisory control and data acquisition) is a category of software application program for process control, the gathering of data in real time from remote locations in order to control equipment and conditions.

Defra is keen for the water industry to consider the public interest in addressing cyber security. Their April 2016 paper laid out a proposal for water companies to work together on a project to develop evidence of ownership of the problem, and steps to improve resilience to cyber threats.

The paper invited companies to consider how to:

- Present evidence to show how the industry has taken ownership of the problem;
- Assess what additional measures they need to improve their resilience to cyber-attacks against a common framework;
- Make the case for investment based on good quality evidence, and include that business case in their PR19 business plans.

In addressing the challenges outlined, the water industry established the CSGP group to review and refine the challenges outlined in the Defra discussion paper and consider a response that would be applicable across the range of water company structures.

1.2 Engagement

Different government departments have responsibilities for cyber security in their respective sectors and administrations. In England, the Cabinet Office owns the National Cyber Security Strategy and Defra is the lead government department for the water sector. Defra is supported by advisors, including the NCSC – which itself provides support to other sectors, such as energy. Defra has a significant role in helping companies manage escalated incidents, regardless of the root cause. This practice helps in supporting any Ministerial communications. Companies can help Defra by keeping Defra informed – in turn, Defra can communicate with Ministers.

1.3 Reporting

In order that the sector can learn, develop and adapt to the evolving risks associated with cyber security breaches, it is vital that reporting routes exist whereby information can be shared with a range of stakeholders. Water companies are working with Defra and its advisors to clarify reporting lines for incidents that escalate above ‘routine’ operations with the aim of establishing a single, consistent approach.

2: About this document

This document is the result of the CSGP group's efforts, and represents the developed thinking of water companies in assessing, preparing and managing the risk of cyber-attack within the industry, together with recommendations for detection, response and recovery. The principles developed here are included in order to provide current thinking of best practice guidance on what water companies could be doing. It includes descriptions of what good looks like, and provides practical examples of where this has been done elsewhere. This guidance has been developed to help companies decide what actions to take and are not prescriptive or intended as a structure for subsequent audit.

The principles assume that companies actively invest in the maintenance of their IT and OT technologies to ensure that they operate securely and are resilient, and that any new investment is 'secure by design'. This has been previously assured through CPNI assessments[2] and is not replicated in this document.

2.1 Scope and purpose

The scope of this work includes OT and IT cyber security readiness.

The document does not prescribe a solution or standard, but offers an unbiased view of what has worked well for others. This is neither exhaustive nor prescriptive, but rather intended to act as an aid to companies in order to support their own cyber security strategies. This will complement activities being undertaken by individual companies to existing standards and practices.

This document does not specifically address retail activities, such as customer billing or data protection, as these are primarily covered by other standards and advice. However, retail organisations may find the contents helpful directly and in their engagement with wholesalers.

2.2 Use of document

This document is meant as a practical guide and indicator of what has worked well for water companies and some other sectors. It is not a technical security document but does reference further technical standards that practitioners can explore.

[2] In future, this role is expected to be taken up by NCSC.

3: Good Practice Principles

The CSGP group has developed six good practice principles with recommendations for implementation, suggestions as to good practice and examples provided by the industry.

The six principles are:

1) To have robust and accountable cyber security governance
2) To manage cyber risk and compliance proactively
3) To ensure all our people are cyber aware with suitable training and communication
4) To make best use good threat intelligence
5) To improve incident response
6) To manage procurement, third parties and the wider supply chain proactively

Table 1 indicates the key parts of existing guidance and frameworks that apply to each of the six principles. This is not meant as an exhaustive list but an indicator of where else companies can go for further information.

Framework	Cross-over and where to go for further information					
Framework	1	2	3	4	5	6
CSGP 6 x Principles	Governance	Risk and Compliance	Training and communication	Threat intelligence	Incidents Response	Procurement and Supply Chain
NIST Categories	Identify , ID.BE-3, ID.GV-1 to 3,	Identify, Protect , ID.RA-6, PR.IP-11, ID.AM-1 & 2, PR.AC-1 & 2, PR.DS-2,	Identify , Protect , Detect, Recover, PR.AT-1 to 5, RC.CO-1,	Identify, Detect, Protect, ID.RA-2, ID.BE-4, DE.CM-4, PR.PT-1,	Protect, Respond , Recover, PR.DS-3 , PR.IP-6, PR.PT-2, PR.IP-9, DE.AE-2, RC.IM-1,	Identify, Protect , Detect, ID.AM-6, DE.CM-4, PR.IP-2, DE.CM-6, ID.BE-1
Cyber Essentials / Plus	Boundary firewalls and internet gateways,	Boundary firewalls and internet gateways, Secure Configuration, Access Control,		Malware Protection,		Patch Management,
ISO27001 Domains	5. Security Policies ,	8. Asset Management , 9. Access Control , 18. Compliance	7. Human Resource Security , 11. Physical Environment , 13. Communications ,	12. Operations	16.. Information security Incident Management , 17. Information Security Business Continuity ,	9. Access Control , 14. Systems acquisition, development & maintenance , 15. Supplier relationships ,
CPNI GPG	9.3.1,	6.3.1, 9.3.1, 4.3.14, 4.3.6,	4.3.12, 4.3.17, 6.3.1, 4.3.6, 4.3.4, 4.3.7,	4.3.18,	5.3.1,	4.3.10, 8.3.1, 4.3.3,

For s more detailed breakdown if CPNI/ISO and NIST see Appendix A.

Table 1: Key parts of existing guidance and frameworks

Principle 1: To have robust and accountable cyber security governance

Introduction

The risk from a cyber event is a business issue and not a technical one. This principle seeks to display strong and clear governance that allows the organisational management of cyber security, but is responsive to problems and issues raised in doing so. Although it is recognised as good practice for all companies to have good governance around cyber security, this is not a 'one size fits all' principle. Companies should consider their risk position and develop proportional mitigation strategies.

Recommendation 1: Create strong governance structures that ensure cyber security is considered and managed, with ownership and accountability from the top of the company

Good Practice includes:

- Minimum Executive level ownership with accountability for the overall cyber risk and mitigation strategy;
- Integration into other Governance structures within the organisation, e.g. Risk Board, business continuity plans and incident response plans;
- Integrated cyber governance that also considers the wider *physical* and *personal* security (persec) threats to the organisation in order to build a balanced management plan and response to threats;
- Regular review of cyber threats, issues and initiatives (recommended to take place at least quarterly);
- Good governance principles and rules which cover both IT and OT security, as well as the wider business;
- Clear organisational accountability for day-to-day management of cyber security (IT, OT and corporate) and defined escalation paths;
- Clear roles and responsibilities for those involved in cyber security governance. Evidenced through clear job descriptions and organisational design. Should include regularly assessing individuals' capabilities within the context of the role they perform;
- Robust assurance processes with good project governance to validate effective security considerations within solutions and change programmes.

Recommendation 2: Develop and maintain policy documents, standards and guidelines

All companies should develop a framework of policies, standards and guidelines for their own use, which can be used to govern cyber preparedness. These documents may be combined, take different forms and/or consist of different formats. However, the documents should be accessible to staff, be reviewed on a regular basis and signed-off by senior executives within the organisation.

Good Practice includes documents that address:

- Security mandate that is linked to company business principles and internal control manual
- Overarching Information Security Policy
- Acceptable use policy
- Secure desk and screen policy
- Document/data classification
- Data protection policy
- Social media/internet use
- Passwords
- Removable media
- Mobile/home-working
- Access Control Policy
- Retention Policies

Principle 2: To manage cyber risk and compliance proactively

Introduction

This principle seeks to demonstrate that risks relating to cyber threats are identified and managed. It is widely acknowledged the threat landscape is changing at a rate faster than most companies can mitigate. The approach to managing cyber risks should be no different from any other risk, and companies should have their own established and documented risk management processes. Such practices will include the reporting of risk within the organisation, allowing others to understand and share in the awareness of cyber risks.

This section is not seeking to identify a best practice risk management process. It seeks to identify good practice to help companies manage the cyber threat, a risk that should be taken equally and seriously within the organisation. Some companies will report against cyber risks, while others will report against information security risks, of which cyber is a potential threat. There is no right or wrong answer and companies should choose the most effective approach for them.

Recommendation 3: Demonstrate that cyber risks are accommodated within the risk management system

Companies must represent the threat to cyber security and the need to prepare and respond at a corporate level should an incident occur (e.g. breach, hack or outage). This risk should be managed by practices of good risk management that clearly identify and manage the risk and are reviewed on a regular basis.

Good Practice includes:

- Recognising the risk of threats to cyber security at a company level, either as a separate risk on the corporate risk register or as a component/actor in another risk such as information security;
- An understood risk appetite which reflects the risk versus investment in cyber security. Regular Executive/Board agenda item;
- A process for validating control effectiveness including understanding systems, threats, impacts and vulnerabilities;
- Understanding where information resides (internally and externally);
- Ensuring information is classified appropriately as part of good information management;
- Have a good and established risk management culture.

Recommendation 4: Develop continuous improvement initiatives aimed at addressing threat, risk and readiness

Good Practice includes:

- Considering a baseline from which improvement can be measured and reported internally;
- Development of the investment case for improving security measures and controls. This should consider setting a current baseline of cyber security readiness, and seeking to prioritise effort to address areas of weakness;

- Delivery of improvement controls and changes for cyber security should be considered within the context of a managed programme of work. This would include clear plans, project risk/issue management and benefits realisation;
- Development of continual communications and awareness campaigns which seek to remind, test and challenge staff behaviours. Finding new ways of engaging with staff and promoting cyber security in everyone's mind;
- Consideration for linking communications for security areas of cyber, physical and persec together to create a set of linked principles, and a mandate for continual information and communication campaigns.

Principle 3: To ensure all our people are cyber aware with suitable training and communication

Introduction

The water industry recognises that behavioural change will help improve the sector's resilience to the cyber threat. Helping staff and partners understand the risks from the cyber threat will drive behavioural change, increase preparedness and thereby increasing resilience to the changing threats.

Recommendation 5: Continue to increase awareness and cyber skills within their wider workforce

The industry recognises the threat posed by the 'insider threat', whether malicious or accidental. Helping the workforce become more aware of cyber security will help mitigate this threat. The application of this should not be limited to employed staff, but the organisation should consider including contractors and third parties.

Make security personal. The CSGP group felt it important to emphasise the success of campaigns which extend cyber security from not just the work place, but to an individual's personal and home life. Helping staff understand the risks and precautions needed when using social media sites such as Facebook and LinkedIn, online banking and email is shown to provide a longer-lasting effect and more direct impact on staff which permeates not just at home but at work too.

Good Practice includes:

- Having an "Acceptable Use Policy" which clearly stipulates what is expected of staff and signposts further information;
- Awareness campaigns, which are multimedia and inventive in their attempt to continually remind the workforce of their duties and the need for diligence;
- Staff inductions, which familiarise staff with the materials and content of the policies which govern information security within the organisation;
- Clear signposting for useful resources, policies and associated information.
- How to recognise and report incidents and near misses;
- Encouraging an openness to report rather than suppress mistakes within the organisation;

- Specialist training courses for IT Security staff, internal audit and other security professionals which help refresh and increase understanding of this changing landscape;
- Testing effectiveness of information campaigns. This might include regular tests such as internal phishing surveys;
- Leveraging relationships with suppliers to make best use of their training, policies;
- Consider ongoing maintenance of cyber awareness and good practice principles including company intranet banners, poster campaigns and annual quizzes with prizes in order to encourage and reward good behaviour;
- Developing a network of coaches and cyber security champions within the business in order to continue the promotion of cyber resilience messages;
- Ensuring that training on cyber security provides the opportunity to seek and answer questions raised by course participants in an interactive way in order to build confidence;
- Ensuring training is developed by professionals (both internal and external) who have current insight into the risks and threats of cyber security;
- Ensuring non-compliance such as failing a training course or not engaging with the awareness opportunities is raised through the governance arrangements (Principle 1).

Principle 4: To make best use of good threat intelligence

Introduction

The ability to understand and recognise threats, including sharing knowledge and awareness with others, making use of both formal and informal channels, are critical to develop good cyber practices.

Recommendation 6: Identify sources of good, reliable and credible intelligence

Identifying sources of good, reliable and credible threat intelligence will help companies be more aware of the threats faced, and the consequences of those threats. This includes proactive sharing between companies and with Defra and the NCSC to help prevent incidents. To include lessons learned, both within and across sectors, to be shared – ideally led by the NCSC (particularly cross-sectoral learning), but recognising the many existing opportunities for water companies to share lessons learned within the sector.

Good Practice includes:

- Engagement with CPNI and NCSC;
- Considering use of external intelligence companies;
- Opportunities to share threat knowledge (e.g. Cyber-security Information Sharing Partnership (CiSP), Water UK networks, Resilience Direct, CPNI, NCSC website);
- Sharing and engaging with wider sector experience;
- Deployment of cyber intelligence and engagement with ethical hackers to reduce the "dwell time[3]" of a breach to well below current levels;

[3] The period of time that a system or element of a system remains in a given state

- Regularly reviewing the changing threat landscape by considering questions such as what are other water companies experiencing, trends in attack within companies, emerging threats in other sectors;
- Needing to understand where the water industry goes for intelligence in the first place. Everyday sources may include: other companies, CiSP/ CERT platforms, internal monitoring tools, BBC website, The Register, paid for external providers, third parties, external incidents etc.

Recommendation 7: Encourage industry knowledge sharing and participation

The water sector is developing different groups that promote participation, both within the industry and across the wider utility sector. The water sector commits to sharing intelligence about protective security good practice, both within the sector and, via the NCSC, across other sectors. Some of these groups are mentioned below however this list is not exhaustive.

Good Practice includes:
Making use of the range of formal and informal networks and platforms, which have a specific cyber security focus, that exist to support the water sector. These include:

- Water UK IT Security Network
- Water Sector Protective Security Working Group
- Water Sector Information Exchange (WISE)
- Defra's Water Sector cyber security governance steering group
- Resilience Direct
- CiSP

Other wider sector groups include:

- Internet Security Fora and professional organisations such as NIST, ISACA and ISC ISF.

Companies may wish to consider additional information sharing with other companies, not just when dealing with an active threat or incident. Consideration should also be given to the rules around top-down and bottom-up sharing of threat intelligence.

Principle 5: To improve incident response

Introduction

Ensuring a proper response to any incident is key to continuation or restoration of services as well as managing reputational and business risk. Companies have business continuity and emergency response plans in place. These plans must recognise that cyber could be the root cause of an incident. Companies may wish to have cyber specific plans, which dovetail into the overall emergency response plan. These plans are as important as actually dealing with an attack or incident and should be understood, rehearsed and revised on a regular basis.

Recommendation 8: Ensure incident response and recovery plans are in place and tested

In order to prepare for an incident which may have a cyber security element, it is important that response plans are developed and tested.

Good Practice includes:

- Developing a cyber security response capability, which could be stand-alone or linked with existing incidence response plans within the company. Examples of the types of questions that companies should address when developing or reviewing a plan include:
    - Is our process adaptable to different incident types? (Denial of service, ransom, phishing, insider theft etc.)
    - Is everyone trained on the response plan?
    - How does our response to cyber specific incidents dove-tail into an overarching emergency response plan?
    - Are operation response teams considering the possibility of cyber-attack as a root cause of failure?
    - Do we routinely test and rehearse the plan? (Including exercises and scenarios).
    - Do we know who the key players are in incident response? And do they know their roles and responsibilities in the response process?
    - Do we have a communications plan with possible pre-scripted messages?
    - How does our cyber security response plan fit with other response plans? How would it be invoked, by whom, when?
    - Who are the key decision makers?
    - Can the company draw on resource for forensic review and assistance during cyber-attack?
    - Does the company have a procedure for tracking of internal and external lessons learned?
- Revising internal policies, procedures and processes to reflect lessons learned;
- Participating in early warning, notification to Defra and the NCSC of suspicion of a cyber incident;
- Plans should be acknowledged and approved by senior company executives who should retain overall accountability.

Principle 6: To manage procurement, third parties and the wider supply chain proactively

Introduction

Outside organisations pose a real and tangible threat to the water industry and its ability to remain resilient to cyber-attack. This may be through partnerships or joint ventures, supply chain or sub-contractors or more informal information sharing arrangement. It is important that the organisation addresses these risks and manages their relationships with all third parties. Consideration should therefore be given to procurement, contract management and supply chain management. This consideration should include both an assessment of the suppliers with greatest risks in both cyber and general information management.

Recommendation 9: Understand the interactions with existing third party service providers and the reach within water company operations

This principle relates to knowing exactly who you are interacting with, and why. The following considers the mapping of third party interactions with your company in respect of cyber (and information) security.

Companies may wish to require third parties to comply with set standards such as ISO27001 and Cyber Essentials Plus. However, all certification should always be backed up by proactive checking and diligence on the part of the company. It is particularly important to check the scope of the certifications to ensure they cover the required activities.

Note: there are time limitations to certifications so checks need to be in place to ensure it covers the full extent of the contract.

Good Practice includes:
The sector should take a joined-up approach to gathering intelligence on:

- Knowledge and awareness of existing third party suppliers;
- Knowing who your suppliers are and how the business interacts with them;
- Knowing what accreditations they have and the scope of those certifications;
- Knowledge of what information the company is exchanging with any third parties i.e. personal and/or business sensitive information as well as access to business critical systems where availability is key e.g. through remote access;
- Making sure all suppliers are risk evaluated and checked accordingly.

Other aspects to consider include:

- Challenging and informing the supply chain about expected credentials and changes in standards;
- The right contractual clauses – building on existing good procurement principles:
    - Right to audit/assure (not needing to provide notice ahead of audit);
    - Right and ability to recover your data;
    - Rights management (e.g. entitlements, not sharing passwords);
    - The need to notify of breach or incident within agreed service level agreements (SLAs).
- Arrangements for remote access to data;
- Business risks associated with purchase of apps, cloud solutions and accepting online terms and conditions.

Recommendation 10: Actively ensure third parties are aware of, and comply with, their obligations and the policies of cyber security within your organisation, from procurement to ongoing contract management

It is essential that your third parties are aware of the current and emerging obligations on them to work within water company policies for cyber security. This should be checked and tested on a regular basis.

Good Practice includes:

- Ensuring all procurement activities account for cyber security both in selection and contracting;
- Ensure the appropriate security controls and measures are detailed in the contract and compliance checks carried out;
- Developing engagement protocols and methodology to ensure third Parties are continually reminded of their obligations and ensure compliance checks are undertaken;

- Ensure contract management continues to take account of your policies in relation to cyber security. This should include contractual clauses which enforce compliance and detail what will happen in the event of non-compliance;
- Ensure third parties are aware of the need to notify you of breaches and cyber security issues within agreed SLAs;
- Ensure contract staff are aware of and understand the need for diligence on cyber security through training and awareness;
- Continued contract management procedures which address the need for rigour around cyber security.

Links and resources

There is a wide range of commercial and third party resources available to water companies. This document provides links to core government advice to prevent any inadvertent indirect endorsement of particular courses or organisations.

Government
Office of Cyber Security and Information Assurance - https://www.gov.uk/government/groups/office-of-cyber-security-and-information-assurance
Cyber Essentials - https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
Scottish Government - http://www.gov.scot/cyberresilience
Cyber aware - https://www.cyberaware.gov.uk/

Official advisory bodies
National Cyber Security Centre (NCSC) - https://www.ncsc.gov.uk/
Cyber-security Information Sharing Partnership (CiSP) - https://www.ncsc.gov.uk/cisp
Centre for the Protection of National Infrastructure (CPNI) - http://www.cpni.gov.uk/

Other frameworks
ISO 27000 suite - http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
US National Institute of Standards and Technology (NIST) - https://www.nist.gov/
Information Security Forum (ISF) - https://www.securityforum.org/

European legislation
The Directive on security of network and information systems (NIS Directive) - https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Useful training resources

There are two courses free online web-courses available from CERT:

- Operational Security (OPSEC) for Control Systems (1 Hour)
- Cyber Security Industrial Control Systems (15 Hours)

https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

The Open University runs a free on-line learning course on cyber:
http://www.open.edu/openlearn/ocw/course/view.php?id=2969

Appendix 1 Water UK Cyber Security Good Practice group

For Water Companies
Ian Bailey, Affinity Water
Phil Chatterton, Thames Water (Chair)
Sarah Clarke, Affinity Water and Defra
Annamaria Cooper, Yorkshire Water
Jim Marshall, Water UK
Paul Smith, United Utilities
Sean Smith, South Staffordshire Water
Tony Smith, Northumbrian Water (Chair of Water UK IT Security Network)

For Defra:
Matt Crossman, Tom Barker, Joe Morely and Moira Redman

For CPNI / NCSC
Russ H, Simon H