Department
for Environment
Food & Rural Affairs

Water Sector Cyber Security Strategy

2017-2021

March 2017

© Crown copyright 2017

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence v.3. To view this licence visit www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ or email PSI@nationalarchives.gsi.gov.uk

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at

wsr.emergencies@defra.gsi.gov.uk
Water Security and Resilience
3rd floor
17 Smith Square
London SW1P 3JR

PB14459

www.gov.uk/defra

Contents

Executive summary

There are credible cyber threats to UK Critical National Infrastructure, including the water sector. These could lead to serious consequences, particularly as increased automation and connectivity reduces the scope for standalone or manual operation of the water supply system.

Recent cyber risk reviews, by government cyber experts, identified significant opportunities for the water sector to operate at a higher-level of cyber security maturity. This is necessary to manage the risks effectively.

This water-specific strategy is part of a government-wide response to the cyber threat, complementing the *National Cyber Security Strategy (NCSS) (2016)*. The strategic vision and objectives have incorporated significant contributions from the sector and aim to guide activities across the sector, including water companies and government. This document also supports Defra's objectives around protection and developing "strong preparedness to respond to emergencies".

The vision for 2021 is **a secure, effective, and confident water sector, resilient to the ever-evolving cyber threat**.

To realise this vision, government and the water sector will work towards the following objectives:

1. **Understand threats:** Build on our joint work to develop our shared understanding of the cyber threats facing the water sector as they evolve.

2. **Manage risks**: Develop and implement approaches to manage risks and address cyber security vulnerabilities in the water sector, now and in the future.

3. **Manage incidents:** Respond effectively, with industry, to any serious cyber incidents, including those that compromise critical water infrastructure.

4. **Develop capabilities:** Government and sector enhance the cyber skills and capabilities of the water sector to meet future needs.

Underpinning these objectives, we will seek to:

5. **Strengthen collaboration:** Strengthen collaboration between government and the water sector and within the water sector.

Water companies must own, understand and manage the risks to their assets, including Critical National Infrastructure. Industry, therefore, has responsibility for the security of their systems. Government will help set the strategic direction and ensure the legal framework supports industry, as well as providing technical advice and, where necessary, training. Industry will need to develop a security-conscious culture amongst staff and third party providers and integrate this into their governance structures.

Introduction

Cyber security presents an enduring challenge for the water sector and other critical infrastructure sectors. The scale and complexity of cyber attacks against the UK is growing and the range of threat actors is widening. The threat is becoming increasingly global and asymmetric. Both state and non-state actors have access to cyber tools that may enable destructive attacks.

This was considered in the *2015 National Security Strategy and Strategic Defence and Security Review*, which highlighted cyber threats as one of the four most serious national security challenges facing the UK, alongside international terrorism, state based threats, and changes in the established international order. Additionally, the *2015 National Risk Register* also identified that the risk of malicious cyber attacks against critical infrastructure is growing.

The *National Cyber Security Strategy* (2016) outlines the government-wide approach to ensure "the UK is secure and resilient to cyber threats; prosperous and confident in the digital world". The Strategy includes the creation of the National Cyber Security Centre (NCSC), which will provide user-friendly expertise for businesses, including water companies.

This *Water Sector Cyber Security Strategy* outlines the shared high-level approach of the water sector and government to address the growing cyber security threat in this sector. It clarifies the vision and objectives, aligned with the government-wide *National Cyber Security Strategy* (2016). This water sector strategy was developed in close collaboration with industry and aims to support water companies in developing their own internal cyber security strategies.

Below this high-level strategy, companies and government will develop more detailed workstreams to achieve the five objectives that in turn should deliver the overall vision. The strategy clarifies the roles of the main groups in addressing the cyber challenge. It will support the development of cyber security capability in the sector, ensuring that organisations will be able to manage the risk as well as be able to recover from compromises. It will also support the sector to develop more mature cyber security, including governance, capabilities and risk management processes, reducing the risk from cyber threats.

The scope of the strategy

Cyber vulnerabilities are easily transferred between organisations. This strategy, therefore, adopts a broad definition of the water sector, encompassing water companies, their supply chains, and representative organisations.

Holistic security encompasses physical, cyber, and personnel security. While acknowledging overlap between the three disciplines, this strategy focuses on cyber security. The strategy encompasses both Information Technology and Operational Technology, recognising the different challenges in each environment.

The strategy was developed specifically for England, but information has been shared with the Devolved Administrations in the development of the strategy.

Strategic Context: Threat and vulnerabilities

The Threat

There are credible cyber threats to UK Critical National Infrastructure (CNI), including the water sector. These could lead to serious consequences, particularly as increased automation and connectivity reduces the scope for standalone or manual operation of the water supply system.

A number of threat actors including terrorists, hacktivists, criminals and foreign intelligence services can use cyberspace as a means to exploit vulnerabilities and cause damage. This could manifest itself in a number of ways, including through the disruption of water supply or affecting the quality of the water supply. Technological developments have increased the attackers' reach and made their identification more difficult.

Cyber threats should not be viewed in isolation. Capable adversaries could also seek to employ cyber methods as part of a 'blended attack' to enable or reinforce a physical attack, or to seek to control industrial plant and control systems at a water plant.

The cyber threat is evolving rapidly as technological advancements increase opportunities for hostile actors. Within the next decade, cyber tools and techniques that are presently the preserve of nation states will be much more widely available and the offensive cyber capabilities of state actors will improve. The possibility of terrorist cyber attacks capable of exploiting vulnerabilities in the UK's CNI and causing disruption is therefore likely to increase if defences are deficient.

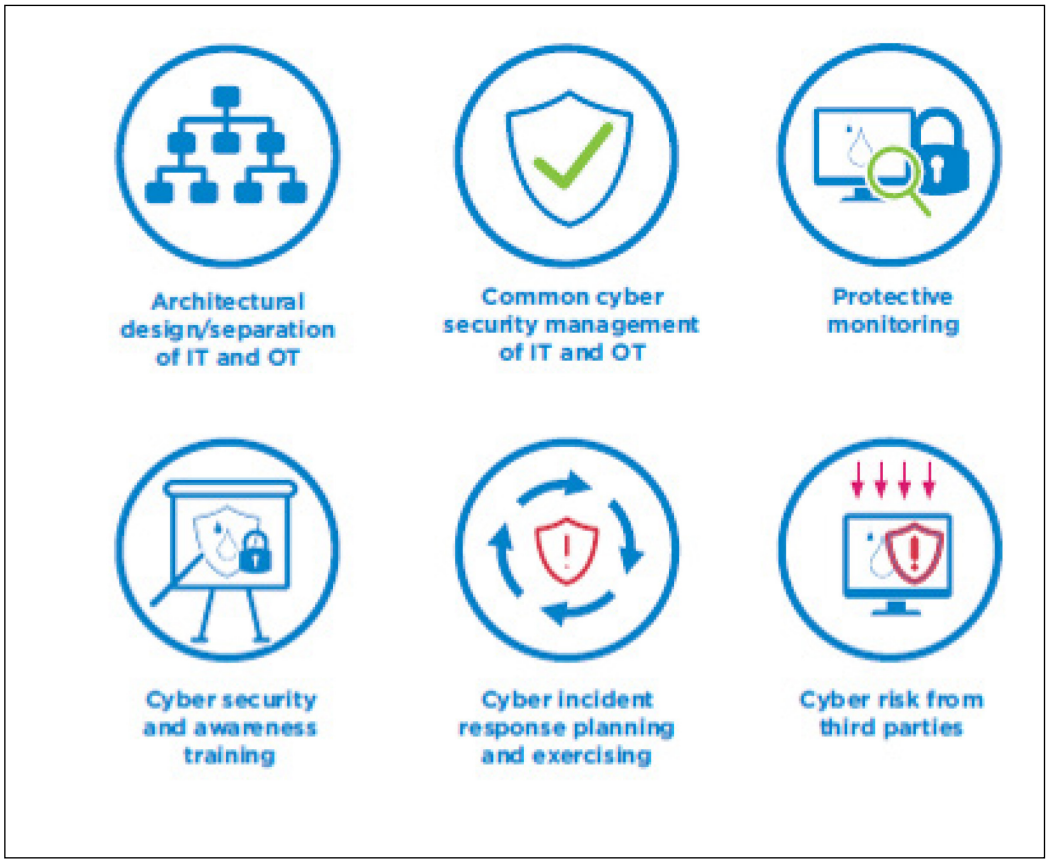
As the threat increases, so too must the industry's ability to defend itself. Over time, exploitation of cyber vulnerabilities in the UK's water sector, either to access and remove sensitive information or support more complex attacks, will become more likely as will the potential for greater resultant impact. The threat extends beyond Critical National Infrastructure could result in significant reputational damage and reduce both investor and customer confidence.

Vulnerabilities

Recent cyber risk reviews, by government cyber experts, identified significant opportunities for the water sector to operate at a higher-level of cyber security maturity. This is necessary to manage the risks effectively.

The ongoing implementation of automated Industrial Control Systems (ICS) with the increasing interconnection of information systems, remote connections with reliance on third party suppliers and integrators has broadened the attack surface of information systems within water companies.

To address these risks the cyber risk reviews identified a number of key areas in which the sector should focus its cyber security activities:



Architectural design/separation of Information Technology (IT) and Operational Technology (OT): Ideally IT and OT systems or networks should be completely separated to prevent infections in IT systems spreading and impacting processes that could cause physical damage.

Common cyber Security management of IT and OT: While IT and OT networks should be separated the two should come under a single set of security policies.

Protective monitoring: Protective monitoring refers to the use of sensors and software to provide information about what is happening within a network or device. Examples of

monitors include intrusion detectors, activity logs and firewalls. Monitoring should be proactive to be effective in detecting malicious activity.

Cyber security and awareness training: Cyber security should not be seen as the preserve of the IT department. Cyber-attacks can target any member of an organisation, and so awareness campaigns for all employees are an effective tool in defending against cyber-attacks.

Cyber incident response planning and exercising: Any organisation needs a set of plans and procedures to implement in the event of a cyber-attack. These plans should set out clear roles, responsibilities and procedures that are easy to follow under pressure. Incident response plans should be exercised regularly to ensure that everyone is familiar with what the plans contain and what their role is within them.

Cyber risk from third parties: Company networks are increasingly accessed by third parties such as equipment suppliers, software suppliers and contractors. Often these entities require the ability to upload software onto systems, make alterations and plug their equipment into the host network. Policies need to be in place to manage this risk, for instance by restricting the number of people with external accesses to a network and ensuring that devices plugged in to the host network are not carrying malware.

The water sector's response

To mitigate the multiple threats the water sector faces, the following vision and strategic approach underpins the water sector's actions in the cyber domain over the next five years.

Vision

Our vision for 2021 is **"a secure, effective, and confident water sector, resilient to the ever-evolving cyber threat".**

- *Secure*- defended against evolving cyber threats and responding effectively to incidents.
- *Effective*- acknowledging that water companies are businesses, cyber security must support the service provided to customers while not unduly increasing costs.
- *Confident*- able to demonstrate to government and other stakeholders, including customers and investors, that cyber security is being properly managed through an effective risk management programme.

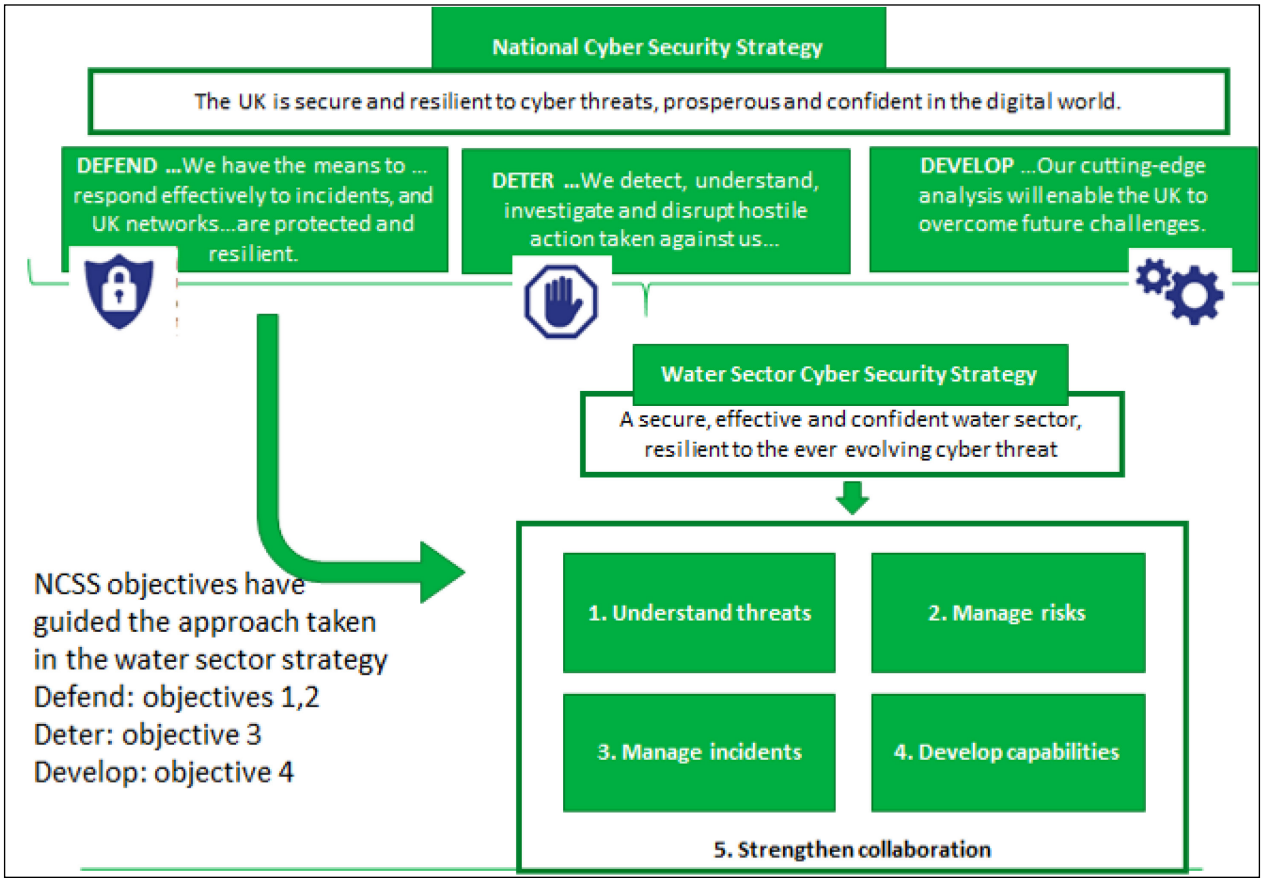
Objectives

To realise this vision, government and the water sector will work towards the following objectives:

1. **Understand threats:** Build on our joint work to develop our shared understanding of the cyber threats facing the water sector as they evolve.
2. **Manage risks**: Develop and implement approaches to manage risks and address cyber security vulnerabilities in the water sector, now and in the future.
3. **Manage incidents:** Respond effectively, with industry, to any serious cyber incidents, including those that compromise critical water infrastructure.
4. **Develop capabilities:** Government and sector enhance the cyber skills and capabilities of the water sector to meet future needs.

Underpinning these objectives, we will seek to:

5. **Strengthen collaboration:** Strengthen collaboration between government and the water sector and within the water sector.



These objectives have been guided by the National Cyber Security Strategy:

It is intended that measures of success will be agreed for each objective.

Workstreams

In working towards these objectives, the government, companies and the wider sector, will develop specific workstreams.

Roles and responsibilities

Developing cyber security for the water sector will require a collaborative approach between government and the water sector. The water sector must fully own, understand and manage the risks to their physical and information assets, including Critical National Infrastructure. The sector, therefore, has primary responsibility for the security of their systems and information. This includes cloud information processing and storage systems that water companies may use.

Government will set the strategic direction and legal framework to support industry, as well as providing technical support, and where necessary, training and advice. Government will share threat information with the sector; define what good cyber security looks like, and continue to address the cyber skills shortage in the country.

Strategic outcomes and delivery

In alignment with the 5 year *NCSS*, this strategy aims to support the water sector develop a mature approach to understanding the cyber threat and produce efficient and effective solutions by 2021. Defra has secured funding from the National Cyber Security Programme to deliver further support and increase capability within the sector.

Water company investments are determined for 5-year Asset Management Periods (AMP), with amounts companies can raise from customers agreed with Ofwat during a Price Review (PR). AMP7 is set for 2020-2025. The Price Review (PR19) process is set to be complete by December 2019. Internal company forecasting is already well underway in some companies. This, alongside Ofwat interim deadlines, means that factoring in any cyber spending could be challenging ahead of the Asset Management Period 7. However, many cyber security measures, such as appropriate governance structures and cultural awareness, have a relatively low financial cost. As the cyber threat is ever-changing, however, it is not possible to discount the need for greater investment not considered as part of PR19.

Measurement

The cyber threat is constantly evolving, which makes measurement on any particular scale challenging. Recent cyber risk reviews, by government cyber experts, identified significant opportunities for the water sector to operate at a higher-level of cyber security maturity. Companies may make significant improvements in security measures over the next 5

years, but this will not necessarily be reflected in an overall improved security maturity score due to the constantly changing nature of the threat. This makes it all the more important that companies continue to improve their cyber security and not fall behind. Thematic measures of success are being developed and will be agreed in due course around each of the five objectives.

Abbreviations

CNI – Critical National Infrastructure. Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

a. Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or

b. Significant impact on national security, national defence, or the functioning of the state

NCSC – The National Cyber Security Centre.

Dstl – The Defence Science and Technology Laboratory

AMP – Asset Management Period. AMP7 is 1st April 2020 to 31st March 2025

PR – Price Review. PR19 is the Ofwat Price review in preparation for AMP7

Glossary

Cyber attack – an attempt to gain unauthorised access to a computer or network, usually remotely

Cyber incident – an occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences

Cyber resilience – the overall ability of systems and organisations to withstand cyber events and, where harm is caused, recover from them

Cyber security – the protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so

Cyber threat – anything capable of compromising the security of, or causing harm to, information systems and internet-connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means

Incident management – the management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.

Incident response – the activities that address the short-term, direct effects of an incident, and may also support short-term recovery.

Industrial Control System (ICS) – an information system used to control industrial processes, such as manufacturing, product handling, production and distribution, or to control infrastructure assets.

Operational Technology (OT) – hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events.

Risk – the potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.