WATER UK

Cyber security preparedness in water utilities in the UK

Dr Jim Marshall, Senior Policy Advisor, Water UK

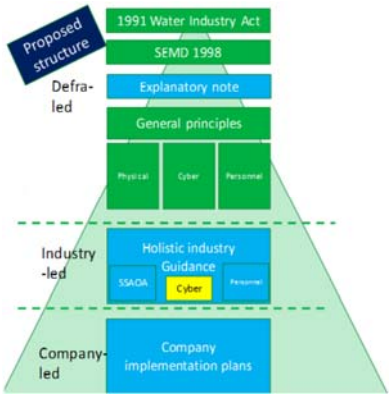
Cyber Water Workshop 2018

Tuesday 9 October 2018

What I am going to cover…

- Tiered approach to cyber security
  - National
  - Sector
  - Company
- Water UK good practice
- NIS Directive

Approach to security in water…



Times they are a changin'

- Period of change – industry under spotlight
  - Cyber risk – generic (data) and specific (ICS / SCADA) → NIS
  - Malicious threats… global, local, disgruntled employee
  - Industry reform .. New players, new activities, new risk
  - Extreme weather – freezing to heatwave in the space of a few months → customers expect service

Tiered structure

National
- National strategy

Sector
- Defra strategy and guidance
- Water UK support

Company
- Plans and procedures

UK National Cyber Strategy

- DEFEND We have the means to defend the UK against evolving cyber threats, to respond effectively to incidents, to ensure UK networks, data and systems are protected and resilient. Citizens, businesses and the public sector have the knowledge and ability to defend themselves.
- DETER The UK will be a hard target for all forms of aggression in cyberspace. We detect, understand, investigate and disrupt hostile action taken against us, pursuing and prosecuting offenders. We have the means to take offensive action in cyberspace, should we choose to do so.
- DEVELOP We have an innovative, growing cyber security industry, underpinned by world leading scientific research and development. We have a self-sustaining pipeline of talent providing the skills to meet our national needs across the public and private sectors. Our cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges.

Defra strategy and guidance

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.

Water UK Cyber good practice

- Established 6 principles for good cyber security
- Supported each with recommendations and examples of good practice
- Intended as a tool for companies to use in building their own cyber security capabilities

Our 6 Principles

- Robust and accountable cyber security governance
- Manage cyber risk and compliance proactively
- Ensure all our people are cyber aware
- Make best use of good threat intelligence
- Improve incident response
- Manage procurement, third parties and supply chain proactively

Principle 1 – robust and accountable cyber security governance

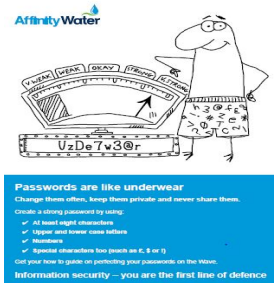
- Recommendation 1: Create strong governance structures that ensure cyber security is considered and managed, with ownership and accountability from the top of the company.
- Recommendation 2: Develop and maintain policy documents, standards and guidelines.

Principle 2 – 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 – ensure all our people are cyber aware

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



Principle 4 – 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 – improve incident response

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

Principle 6 – manage procurement, third parties and 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.

NIS Directive (EU2016/1148)

or "measures for high common level of security of network and information systems across the Union)

- The Directive is not just cyber but covers all risks to networked service provision or where network failures can impact service
- Requires establishment of national operators of essential services
  - Each MS to identify the entities subject to security and notification obligations → where a cyber incident could have significant disruptive effect
- Operators of essential services required to adopt security requirements to:
  - Prevent risks
  - Ensure security appropriate to risks
  - Handle incidents – minimise impact
- Notification to competent authority of "incidents having a significant impact on the continuity of essential services" +voluntary notifications of other

NIS Directive - structure

- NIS Directive words suggest four key overarching objectives that help structure any set of cyber security principles.
- Organisations that deliver essential services should have:

A. appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to essential services;

B. proportionate security measures in place to protect essential services and systems from cyber-attack;

C. capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services;

D. capabilities to minimise the impacts of a cyber security incident on the delivery of essential services including the restoration of those services where necessary.

- The objectives usefully align with the NIST Framework top-level functions IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

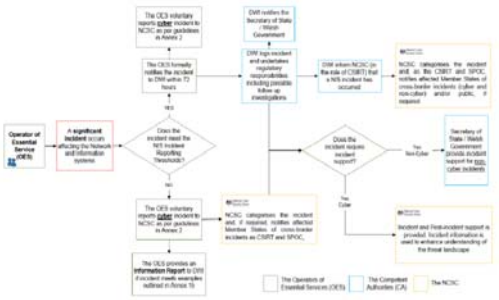
NIS Content

National Cyber Security Centre

NIS Directive Objectives And Principles

A. Organisational Capabilities	B. Protective Security Measures	C. Attack Detection	D. Incident Response
Governance	Policies & Processes	Security Monitoring	Response & Recovery Planning
Risk Management	Identity & Access Control	Proactive Security Event Discovery	Lessons Learned
Asset Management	Data Security		
Supply Chain	System Security		
	Resilient Networks & Systems		
	Staff Awareness & Training		

Incident reporting – what's in or out of scope is a big question



Summary and conclusions

- Collected set of strategy, guidance and good practice working towards our vision
- Talked about government, collaborative sharing, impact of NIS
- Outcome - Secure, proportionate and trusted water sector providing an essential public health service