WATER UK

A secure, effective and confident water sector, resilient to everchanging cyber threat

Dr Jim Marshall, Senior Policy Advisor, Water UK

Cyber Water Workshop 2018

Monday 8 October 2018

What I am going to cover….

- Role of the water sector as critical national service
- What we mean by security
- Why worry?
- Risks
- Holistic approach
- Where do we need to be?
- How are we getting there?

What is the role of the water sector?

- Production of clean, wholesome drinking water and safe removal and disposal of waste
- Process driven
- UK water industry is effectively fully integrated with risk-based plans
  - Source to tap approach to drinking water (DWSPs)
  - Toilet to see approach to waste water (DWMPs)

Water is critical to the nation… as is the infrastructure needed to deliver it

- The UK's Critical Infrastructure is defined by the Government as:

'Those critical elements of Infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life'

- Some water and waste water assets fall into this category – security standards and requirements set by govt
- Some water and waste water assets don't – set our own UK water industry standards

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf

What do we mean by…

- Secure – protected against threats from individuals or organisations aiming to interrupt this process by physical, cyber or human means
- Effective – an industry that is able to improve process and service by adopting new technology to replace or improve existing
- Confident – people can turn on the tap and access water without any concerns over its safety

Do we need security or resilience?

- Security - reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.
- Resilience - as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incident

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

Or more simply

- Security = protection and prevention
- Resilience = ability to carry on

Security of water services

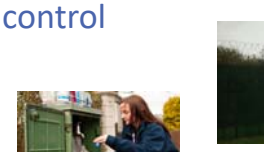
- Securing the water treatment, distribution and wastewater collection, treatment and disposal system to protect integrity of the system
  - Impact of not doing so – risks to public health, consumer confidence or environment
- Securing customer data and corporate information that water companies use for their business
  - Impact of not doing so – data regs breaches, commercial risk

Why worry?

- Increasing risk of intentional damage to water supply or water supply systems by persons for malicious reasons – water industry having to do much more to protect an essential service
- Climate factors are also becoming more important – extremes of wet and dry periods
- Impact on ability to customers → health

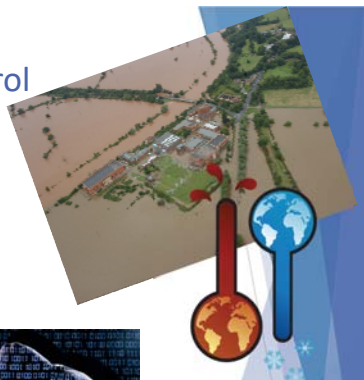
Risks within our control

- OT / IT up to date
- Protected IT
- Site security
- Network / quality
- Staff employment

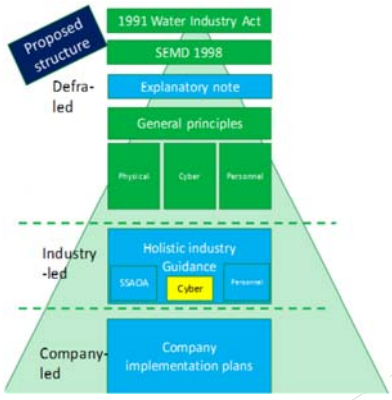


Risks outside our control

- Loss of electricity
- Loss of chemicals / supply chain
- Widespread flooding
- Climate change
- Extreme weather
- State action
- Global conflict

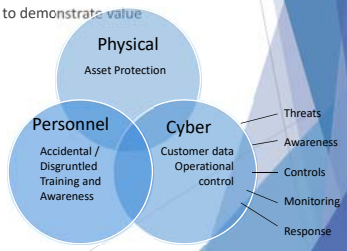


Approach to security in water…



Taking a holistic view of security

- Security can't operate in isolation
- Think holistically
- Traditionally focussed on physical protection
  - Fences and alarms are tangible and easy to demonstrate value
  - Cyber counter measures less so
- New challenges



Physical security measures….

Aim: to prevent access to sites, infrastructure or critical locations

- Fences
- Locks
- Access control
- CCTV
- Asset resilience / service resilience

Electronic security measures….

Aim: to prevent unwanted access to or damage of electronic information or control systems

- Patching strategy
- Firewalls / air gaps
- Device control
- USB control

Human security measures….

- Aim: to ensure that people are aware, that the right people are doing the right jobs, prevent insider actions, deliberate / unintentional distribution of viruses
-
- Vetting / screening
- Job specific access
- Workstation policy
- Training – operatives / teams
- Awareness

Assess, audit and appraise….

Water Sector

Department for Environment, Food and Rural Affairs

The Department for Environment, Food and Rural Affairs is the Lead Government Department responsible for Water sector CNI and for managing any risks.

An all risks regulatory framework, effective mutual aid arrangements and high levels of investment continue to strengthen the resilience of the water industry to major disruptive events.

Assessment of Existing Resilience

- Irrespective of the risk, water companies are required by law to plan to provide water by alternative means in the event of a failure of the mains supply.
- The piped water supply system is generally resilient to the loss of individual facilities, and there is a widespread ability to reroute supplies from other parts of networks.
- However, disruption to electricity supplies or widespread flooding could result in the loss of mains water and affect the movement and treatment of sewage. Water companies have contingency plans in place which include the use of back-up generators.
- Emergency response is bolstered by industry-wide and local mutual aid agreements to enable the sharing of resources between companies.
- All companies maintain statutory plans to minimise the impact of a drought.

But we need to continually improve…..

What does a secure sector look like?

- All risks mitigated at any cost?
  - Probably not
- Threats identified and risk assessed- most likely protected
  - Probably
- Balance the likelihood against the impact
  - Data breach – rare but big impact
  - Service break – more regular, less customer impact

How do we get there?

- Assess risks – shared risks, joint learning – in it together
- Invest in appropriate capital but also make sure we have the right people doing the right jobs
- Be open to evolution
- Understand the impacts
- Consider resilience as a security measure?

What happens if we get it wrong….

- It's a public essential service without it:
  - People get sick or lose trust
  - Businesses lose money
  - Politicians get involved
  - Investors move on
- Without trust and without confidence the sector will not be able to do its job
- People expect water to be safe
  - – its our job to make sure it is

But when we get it right…..

Summary and conclusions

- The provision of drinking water is an essential service – vital for health and well-being
- Like any process based system it has vulnerlabilities that could be attacked / exploited
- Our role is to assess, understand and protect these wether it be by physical, electronic or personnel approaches
- We want this system to be secure but it also needs to be effective and proportionate
- Cyber is a developing threat – we need to evolve with it