Chapter 10
Information Security Threats of Automation in the Water Industry:
An Exploratory Study of England and Wales

James Taylor
Bournemouth University, UK

Festus Adedoyin
https://orcid.org/0000-0002-3586-2570
Bournemouth University, UK

ABSTRACT

Critical infrastructure is reliant on automation to efficiently deliver services. Supervisory control and data acquisition (SCADA) systems monitor and control the operational network and these devices can be compromised with a cyber attack. This report evaluates the significance of such threats, the economic impact, reviews foreign ownership of critical infrastructure and the current legislation as it relates to the water industry. The report concludes with potential recommendations the United Kingdom might consider protecting this vital service.

INTRODUCTION

Cyber warfare is being actively waged, and the opportunity to disrupt another nation-state is being fought over the internet. As was witnessed in 2010 when Stuxnet delivered a worm that disrupted Iranian nuclear enrichment research in Natanz. Specifically infecting Siemens controllers within Iran and preventing them from doing anything useful (Langner 2011). More recently, in 2015, BlackEnergy notoriously infected the Ukrainian power grid causing power outages for more than 6 hours. The US Department of Homeland Security has discovered BlackEnergy malware within their national critical infrastructure,

DOI: 10.4018/978-1-6684-9018-1.ch010

including nuclear power plants, oil and gas pipelines as well as water filtration systems (Khan et al. 2016). Both attacks were focused on digitally connected automation controls.

SCADA is part of the wider Industrial Control Systems (ICS) or Operational Technology (OT), and many industries use SCADA controls to automate the delivery of their services. Critical National Infrastructure (CNI) such as the electricity grid, rail services, telecommunications and water services all make use of SCADA controls. A deliberate attack on these services in times of conflict amounts to cyber warfare (Nicholson et al., 2012) and as such, the nation must be assured of minimal disruption. This chapter explores SCADA deployment within water authorities in England and Wales, the implications of a cyber-attack, the economic impact such an attack may have as well as the current legislation to encourage cyber resilience. The chapter concludes with recommendations the industry could consider assuring the nation, vital services are delivered as expected.

Within the water utility sector, SCADA provides automation for a wide variety of uses. Monitoring and controlling pumps, valves and filters used in the treatment of water, with similar controls in the management of sewage. SCADA can also be used in monitoring the physical security (e.g., CCTV, alarm systems, and so forth) of remote locations as part of the overall security considerations, protecting plant equipment from tampering, theft, or damage. With the advancement of the industrial internet, more automation is possible. OT needs to be rigorously managed as the potential for actual physical harm is possible; if the attackers compromised water purification processes and produce false readings on water testing devices, this could prove fatal to consumers.

IT and OT share similarities and both teams should share resources (Desai 2016). This convergence of technologies will present security vulnerabilities requiring both disciplines to proactively work together. IT still has many responsibilities securing the privacy of their customers and whilst this paper is focused on protecting OT, it has been known for attacks on consumer data to be launched via vulnerabilities in OT, such as the data breach with Target whereby access was gained through the heating and ventilation systems (Committee on Commerce, Science, and Transportation 2014). Unfortunately, SCADA lacks basic security controls and therefore is exposed to threats and vulnerabilities (Singh, 2022). This was recently highlighted at the Pwn2Own Championships, where the hackers noted the SCADA challenges were the easiest yet (O'Neil, 2022).

To understand the threat, it is worth considering the likely threat actors. Nation states committing cyber warfare, socio-political groups furthering their cause through cyber terrorism or even possibly a disgruntled employee looking to disrupt operations. Or in the case of an Irish water treatment facility, crypto miners leverage computing power to mine cryptocurrency (Thomson, 2018). In reality, due to the anonymity of the internet, "cyberspace is unknowable" (Barnard-Wills & Ashenden, 2012). It is possible to assume who the likely threat actors are, in the case of Stuxnet and the Ukrainian BlackEnergy attacks, one could conjecture nation states were responsible; however, this is not proven. Whilst it is virtually impossible to regulate the internet or pursue e-criminals, the only course of action is to ensure a robust and resilient approach to all potential threat actors.

Threats and vulnerabilities and the associated risk of SCADA usage are considered below alongside possible mitigation strategies: Internet Exposure: Does the control need to be internet enabled? Just because it can, does not mean it should; Poor Network Segregation: Segregation of duty is a well-founded cyber principle, as was the case with Target the IT systems were compromised via OT; Default configuration: Thousands of controllers are deployed across a SCADA network, whilst it may benefit the operator to keep access simple, the default options must be changed, for example, Admin / Admin;