International Journal of Engineering Management
2020; 4(1): 11-16
http://www.sciencepublishinggroup.com/j/ijem
doi: 10.11648/j.ijem.20200401.12
ISSN: 2640-1525 (Print); ISSN: 2640-1568 (Online)

Water Industry Cyber Security Human Resources and Training Needs

Richard Skiba

LRES Training Management, Melbourne, Australia

Email address:
richard@skiba.com.au

To cite this article:
Richard Skiba. Water Industry Cyber Security Human Resources and Training Needs. *International Journal of Engineering Management*. Vol. 4, No. 1, 2020, pp. 11-16. doi: 10.11648/j.ijem.20200401.12

Received: June 28, 2020; **Accepted**: July 15, 2020; **Published**: July 23, 2020

Abstract: Cyber-attacks are a growing and persistent threat to water infrastructure, including drinking water and wastewater systems. Water infrastructure uses a number of technical control systems to manage and track infrastructure properties, including hardware and software, such as monitoring and data acquisition systems, process control systems, and other devices, such as programmable logic controllers, that control data gathering equipment and information technology. As these systems become more connected to corporate systems and the internet, security approaches are needed equally across both the control system and the corporate network infrastructure, as there are many potential entry points for cyber attackers to exploit to these systems. These cyber-attacks occur on water infrastructure world-wide and water providers, in order to reduce the risks, need to identify control system asset security vulnerabilities and design, build and maintain a security architecture proportionate to the risk. Human resources are fundamental to these cybersecurity systems and the required emerging job roles require industry specific definition. This paper provides definition on the roles and responsibilities for control system security governance, particularly from the perspective of skills and knowledge and training requirements with a view to addressing leading industry security standards for control systems and practices.

Keywords: Cyber Security, Cyber Attacks, Risk Mitigation, Critical Infrastructure, Water Industry, Scada, Supervisory Control and Data Acquisition

1. Introduction

Australian industry Standards [1] identifies that the "growing pace of new innovations and technologies is accompanied with increasing exposure to cyber security threats" and identifies that water technologies and innovations such as Big Data, IoT, and automation create large amounts of data potentially exposing the industry to growing cyber security risks. The same report notes that development of skills and capabilities through training and educational programs is a key to understanding cyber security and protection from cyber security threats. Similar needs are noted in the United States, with the 2019 AWWA State of the Water Industry report identifying that a "robust and tested cybersecurity program is critical to protect public health and safety, prevent service disruptions, and safeguard customer and employee personal and financial information [2]". Germano [3] concurs noting that cyber security is a top priority for the water and wastewater sector and considerable attention and resources directed to cybersecurity preparedness and response are required. Department for Food and Rural Affairs [4] identifies that cyber security threats are becoming increasingly global and asymmetric. Cyber-attacks can potentially impact in water system ranging from overflowing dams to water contamination, to the ultimate failure: loss of human life.

Effective cyber security requires both good technological solutions and good people solutions [5]. The role of training in the development of these components, particularly within the water industry, forms the focus of this study with attention to identification of the human resources aspects of cyber security for water industry infrastructure operators.

2. Method

An exploratory research method, primarily utilizing semi-systemic literature review, is applied as a method to this study, where, as outlined by Snyder [6], a literature review can

broadly be described as a more or less systematic way of collecting and synthesizing previous research. Previous research is reviewed and analyzed to describe research area including establishing current cyber security needs in the water industry and the various roles played by training to meet these identified needs. The study explores collective evidence to discuss an approach to effectively manage the risks associated with cyber-attacks. The applied approach aims to contribute to the creation of critical infrastructure organizational guidelines for policy and practice to best protect their key assets.

3. Discussion

3.1. Emerging Cyber Security Needs in the Water Industry

Germano [3] illuminates that a cybersecurity attack on critical water sector operations could cause "devastating harm to public health and safety, threaten national security and result in costly recovery and remediation efforts to address system issues as well as data loss".

The Victorian Auditor-General's Office [7] outlines that water control systems are increasingly the target of cyberattacks worldwide, citing examples including results from audits of water and energy systems undertaken in Queensland and Canada respectively, and an annual review by the United States of America's (USA) Department of Homeland Security. The audit completed by the Victorian Auditor-General's Office concluded that Victorian water providers lacked "a strategic approach to managing cybersecurity risks that integrates their corporate and control system environments and aligns to leading industry security standards for control systems [7]". They further found that while the audited water providers have actively improved the security of their corporate systems against cyberattacks, the evolving threat landscape requires an increased focus on assessing and significantly strengthening control system security.

Water infrastructure utilizes a range of technological control systems to operate and monitor infrastructure assets including hardware and software that controls equipment and the information technology that gathers data. This includes supervisory control and data acquisition (SCADA) systems, process control systems, and other devices such as programmable logic controllers [7]. These systems allow remote monitoring and management of the infrastructure assets. As these systems become more connected to corporate systems and the internet, security approaches are necessary equally across both the control system and corporate network infrastructure as there are many potential entry points to these systems that cyber attackers can exploit.

At a fundamental level, the American Water Works Association [2] outlines that a number of basic factors increase water infrastructure vulnerability to cyber-attack such as insufficient antivirus protection and network security tools. These tools can include use of network security devices including grades of equipment utilized. As an example, utilization of residential grade routers and firewalls rather than commercial equipment requiring specialist skills to install and operate. Other vulnerabilities are included in network equipment manufacturer exploitable services, included in equipment to allow manufacturers to access the equipment for purposes of updating, fault finding and maintenance, performed remotely. Failure to change vendor default settings, enhance security and regularly patch systems and software can further introduce vulnerabilities, as can neglecting network devices when assessing risk or recovering from a cyber intrusion. The American Water Works Association [2] explains:

"The reality and prevalence of cyber risk mandates that organizations and their leaders not only take meaningful action to prevent and detect harms, but also have a tested plan for responding swiftly and effectively when cyber incidents do occur. Failing to address cybersecurity risk in a proactive way can have devastating results".

A range of technical and procedural security measures can help protect against many cyber threats [2]. There are a broad range of occupational taxonomies that are responsible for their application. These include Network Supervisors, Hydrographers, Work Planners, Trade Waste Officers, Hydrometric Monitoring Officers, Section Coordinators, Salinity Interception Officers, Supervisors, Groundwater Extraction Coordinators, Reticulation Coordinators, Dam Safety Instrumentation Specialists and Dams Operations Coordinators [8]. Those in these job roles at the very least, must comply with basic standards related to network administration and cyber security including restricted physical and technical access, firewalls, logging and encryption. The Victorian Auditor-General's Office [7] notes that there are not clearly defined and documented roles and responsibilities for the security of these systems within the Victoria water providers audited.

A recent study presented a review of fifteen cybersecurity incidents in the water and wastewater sector covering a wide variety of vulnerabilities and situations from the Maroochy Shire Sewage Treatment Plant insider attack in 2001 to the Riviera Beach Water Utility ransomware attack in 2019 [9]. The study found that the sheer diversity of the systems, attackers, and consequences associated with the incidents indicate a need for inclusive and comprehensive vulnerability assessments, as well as risk mitigation, preparedness, response, and recovery studies that account for such extreme heterogeneity. This highlights the need for specialist training and human resource requirements that are able to develop and implement cyber security systems across not only corporate network infrastructure but also specifically related to SCADA systems utilised in water assets.

3.2. Passive and Active Cyber Security Activities

Masud [10] identifies that, until recently, cybersecurity programs have centered on passive defence activities such as network isolation and segmentation. These activities are primarily designed to mitigate system vulnerability and generally do not require human intervention. Passive security

countermeasures can include application of anti-virus software, security patches, signature-based intrusion detection systems, email filters and firewalls [10]. In recent years, water utilities have recognized the importance of installing, improving and keeping these systems up to date to mitigate the risk of cyber-attack. These passive systems can leave water systems susceptible to sophisticated and targeted attacks. Masud [10] notes that "an agile and active defense strategy is required to stay ahead of the most advanced adversaries". This requires applying a cohesive cyber security strategy that is applied to all aspects of the operation in an ongoing manner and in parallel with all business operations throughout a utility's lifecycle.

Active defence activities require dedicated human resources for their continuous and ongoing application, providing sophisticated organizational forensics and intelligence development and sharing. To effectively secure process control system networks, such as SCADA systems, a multistage process is needed incorporating risk assessment, planning, design, implementation, and maintenance for a comprehensive defence-in-depth strategy [11].

3.3. Training Requirements

Bartlett and Northcott [12] discuss the benefits of a consistent operator competency standard in the Water Industry. They suggest that the industry can benefit from a common benchmark to underpin the minimum knowledge, skills and experience required for frontline operator roles. The produced benefit being nationally consistent approach that would assure regulators, water utilities, customers and communities that the frontline operator workforce is capable and competent to deliver water service obligations. They also note that:

"A lack of training and competency provision can reside as a vulnerability within an organization's system, waiting for the right circumstances to present and test frontline operator competency [12]".

Victorian Auditor-General's Office [7] notes that there are not clearly defined and documented roles and responsibilities for the security of these systems. Further, Brumfield [13] notes that water utilities around the world, are vulnerable to attacks because they are usually small and have almost no cybersecurity expertise among staff members. Cybersecurity training is also critical and policies on mobile and 'bring your own' devices must be developed and enforced. In discussing cyber security for the African water system, Amengor [14] identifies that routine training has to be organized for employees to sensitize them on their role in preventing and reducing cyber threats and that staff dedicated to cyber security need to be current with the latest cyber risks and solutions to mitigate and respond to cyber-attacks effectively. Amengor [14] highlights informed people as a fundamental component in securing the African water system against cyber-attack.

Addressing control system security poses different challenges due to the specialized hardware and software, and the need to maintain reliable, available, and supportable services [7]. A range of specialist skills are required to install, configure and manage this hardware and software. The Victorian Auditor-General's Office [7] refers to the US based National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and a guide to control system security, NIST Special publication 800-82. This framework and guide specify a risk - based approach to managing cybersecurity for critical service providers and can serve as a basis for determining the knowledge and skills required to manage cyber security threats in the water industry. They provide an overview of five key functions in cybersecurity risk management headed as identify, protect, detect, respond and recover. Identification requires determination of the resources that support critical business services, their assets, and security risks. Protection requires the development and implementation of safeguards to ensure delivery of services. Protection includes access control, awareness and training and data security. Detection allows for development and implementation activities required for monitoring and detecting cyber security incidents and response facilitates taking action to a detected treat. Recovery allows for the development and implementation of plans for resilience and to post cyber security incident restoration of services.

The American Water Works Association [2] outlines that in partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology Information Sharing and Analysis Center (ISAC), the Water Information Sharing and Analysis Center (WaterISAC) has developed a list of 10 basic cybersecurity recommendations that water and wastewater utilities can use to reduce exploitable vulnerabilities and defend against avoidable data breaches and cyber-attacks. These recommendations include maintenance of an accurate inventory of control system devices and eliminate any exposure of this equipment to external networks. They also include utilization of network segmentation and firewalls. In terms of user access and control secure remote access methods must be utilized with strong passwords and changed default passwords. Patches and updates should be consistently applied.

For general employees, there are several cyber security awareness topics that should be taught, as outlined by Zoe [15]. These include outlining: the range and forms of cyber security threats; the importance of password security; email, internet, and social media policies; protection of company data; and identification and reporting of cyber security threats. This training is generally 'in-house' and should be included in the induction program for employees in the water industry.

Overview of cyber security threat training should include at the very least methods to identify spam content that can contain malicious software, such as can be embedded in email, social media messaging and a range of other platforms including invitations, such as through LinkedIn [15]. The notion of phishing and related cams also needs to be addressed, including typical sources and the types of information phishing seeks, such as usernames, passwords or financial or personal information. Pathways for downloading ransomware

and malware must be highlighted through the training. Finally, Zoe [15] highlights, social engineering, where cyber criminals disguise themselves with fake but trusted online identities to trick employees into handing over sensitive information, must also be addressed in the training. Importance of password protection and password security needs to be explained at this level of training, as do the policies for safe use of email and social media. The rules for safe browsing are fundamental to a training program of this nature. Zoe [15] further outlines that Information security training should describe the regulatory and legal obligations of data protection. Reporting of identified threats is key to managing the threats. Employees need to be aware of the processes they should follow to report red flags, as well as the right people to talk to about suspicions of a cyber-attack.

Brook [16] identifies that most employees understand the vital nature of the systems and how to operate and monitor controls, however many who operate SCADA systems are undertrained in preventing, monitoring, and identifying potential threats to security. Cyber security awareness training is critical for these staff.

Aside from delivery of these programs as part of an induction for new employees, they should also be provided as refresher training to existing staff. These types of training programs contribute to active cyber security as outlined by Masud [10] and address some of the key areas identified by American Water Works Association [2]. Creating awareness about online security threats should be mandatory in water industry organisations given the critical infrastructure they provide.

Water infrastructure organisations also require cyber security specialists to establish and monitor the secure environment. In Australia, the Vocational Education and Training (VET) system provides qualifications for occupations involved in water industry operations, treatment of drinking water and wastewater, and irrigation. These qualifications ranging from Certificate I through to Diploma cover a range of water industry occupations including generalist, treatment, networks, source, irrigation, hydrography and trade waste [1]. These qualifications define operator competency standards and provide a benchmark for competency of operators in the industry. These qualifications do not currently include specific units of competency, or competency standards, for water industry cyber security.

These roles require a high degree of technical proficiency to adequately provide knowledge and skills to protect the organization and infrastructure from data breaches and attacks. These roles can include security architect, security consultants and penetration testers or ethical hackers. Generally, security architects design, build and implement network and computer security for an organization and are accountable for creating complex security structures and ensuring that they function properly. These roles should be professional roles, generally requiring a bachelor's degree in computer science, information technology, cyber security, or a related field to possess the required knowledge and skills. Irrespective of the qualifications, employees in these roles must have the required knowledge and skills to manage cyber security related to SCADA such as is applicable to water infrastructure operations. Industrial Control System (ICS) training is essential to this role where it is performed in the water industry.

Training in Industrial Control Systems will allow the security architect to understand and evaluate the vulnerabilities specific to critical Infrastructure and appreciate the principles behind the industrial hardware and software of control systems used in the operation. In turn, they can then develop and implement mitigation strategies and the associated administrative and technical risk management plans to protect and secure the process control systems. This includes an understanding of Distributed Control Systems (DCS) that are used to control production systems within the same geographic location for industries such as oil refineries, water and wastewater treatment, electric power generation plants, chemical manufacturing plants, automotive production, and pharmaceutical processing facilities [17].

Security consultants, or sometimes referred to as information security consultant, computer security consultant, database security consultant or network security consultant, may also be utilized to assess cybersecurity risks, problems and solutions for the organization and guide them in protect and secure the assets. These roles, as for security architects, may require additional training to encompass SCADA. Training also needs to include applicable standards, where these are in place. As an example, in 2016, the European Union developed the Network and Information Systems Directive (NIS Directive) to improve the security and resilience of control systems for critical services across all member countries. The NIS Directive requires the adoption of IEC 62443—Security for Industrial Automation and Control Systems as a mandatory standard, and this has been implemented in the United Kingdom [7].

Other organizational roles in a critical infrastructure environment can include penetration testers, also referred to as ethical hackers, who search for weaknesses in information technology systems, networks and applications using the same knowledge and tactics as criminal hackers. This role requires simulating real-life cyber-attacks, identifying vulnerabilities and assisting organizations to strengthen their security measures.

Current need for of suitably qualified and skilled human resources, training, and secure control systems and processes are highlighted by the statistics based on the CyberX 2019 Global ICS & IIoT Risk Report. as noted by ELEKS Operations OU [18]. These include identification that 40% of industrial sites have at least one direct connection to the public internet, 53% of sites have obsolete Windows systems such as Windows XP, 69% of sites have plain-text passwords traversing their ICS networks, 57% of sites are not utilizing anti-virus protections that update signatures automatically, 16% of sites have at least one Wireless Access Point and 84% of industrial sites have at least one remotely accessible device. A large number of industrial sites, on this basis, are vulnerable to cyber-attack.

3.4. SCADA System Security Requirements

SCADA systems are used to remotely monitor and control processes that are critical such as factory processes, utility plants and remote locations such as mines, pumps and power generators, using sensors for data collection, management and control. SCADA security is related to protecting these industrial control systems. There are range of specific threats to SCADA networks including hackers, malware, terrorists and employees. Employee threats may stem from human error or disgruntled employees. SCADA security must effectively address this full range of threats. Daalder [19] outlines the most common vulnerabilities in SCADA systems include improper input validation, permissions, privileges and access controls and improper authentication.

The first layer of defence in these systems, as outlined by Daalder [19], is related to physical protection. Water industry cyber security experts must be able to provide system hardening in this context and develop organizational security regulations to mitigate these risks. Given SCADA has developed into a geographically distributed system, risk mitigation, as a second layer of protection, is required whereby the networking environment allows users to only access the assigned dedicated areas. This approach may, for example, utilize dedicated Virtual Local Area Networks (VLAN) to decrease the risk of vulnerability in case of a cyber-attack [19]. Traditional approaches such as firewalls and Demilitarized Zones (DMZ) may also be used. IEC 62443—Security for Industrial Automation and Control Systems provides guidance that may be implemented by security architects for system design in this regard. Virtual Private Network tunnel (VPN) allow the integration, authorization and authentication of data transactions between various networks with private use of the public network. Transactions through a VPN can reduce the vulnerability of a cyber-attack.

Other controllable vulnerabilities are inherent in the technology used. As an example, Object Linking and Embedding (OLE) for Process Control (OPC) is a generally accepted open protocol within the Process Control Industry [19]. Typical OPC makes use of Distributed Component Object Model (DCOM), a Microsoft technology for application communication between machines across a network. DCOM services are normally open to allow ease of use of client software, typically in office environments. Use of OPC Tunnelers enables SCADA systems to communicate with OPC-servers without transporting OPC-protocol over the underlying networks and may be used to minimise cyber-attack risks resulting from this vulnerability. Data transfer across the internet where there is a degree of separation between network components may also be create vulnerabilities. Use of Secure Sockets Layer (SSL), or Transport Layer Security (TLS), provides message encryption, detection of message alteration and authentication between the client and server, which in turn reduce the risk of interception.

This SCADA system vulnerability overview highlights some of the differences between mainstream networks and SCADA systems, such as utilized in the water industry. SCADA environment cyber security requires a range of specialist skills applicable to complex system requirements to account for these differences.

4. Conclusion

Protection of water and its delivery requires protecting data and systems, and cyber security has a vital role to play in conserving and delivering a safe water supply. Effective cyber security extends beyond the installation of software and hardware protective systems. It requires a range of specific human resources with an in-depth knowledge of the particular operation and the technology it utilizes. As a matter of priority, critical infrastructure operators, such as the water industry, should engage a dedicated SCADA security team to prepare and implement an effective cyber security defence plan utilizing secure architecture and processes.

References

[1] Australian Industry Standards. (2019). Water Industry Reference Committee: Skills Forecast 2019. Retrieved from https://www.australianindustrystandards.org.au/wp-content/uploads/2019/06/nwp_sf2019_final_pages_low_res.pdf.

[2] American Water Works Association. (2019). 2019 AWWA State of the Water Industry Report. Retrieved from https://www.awwa.org/Portals/0/AWWA/ETS/Resources/2019_STATE%20OF%20THE%20WATER%20INDUSTRY_post.pdf.

[3] Germano, J. H. (2018). Cybersecurity Risk & Responsibility in the Water Sector. Denver, CO: AWWA. Retrieved from www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf?ver=2018-12-05-123319-013.

[4] Department for Food and Rural Affairs. (2017). Water Sector Cyber Security Strategy: 2017-2021. Water Security and Resilience: London.

[5] Australian Computer Society. (2016). Cybersecurity: Threats, Challenges, Opportunities. Australian Computer Society: Sydney.

[6] Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039.

[7] Victorian Auditor-General's Office. (2019). Security of Water Infrastructure Control Systems. Victorian Government Printer.

[8] Department of Education, Skills and Employment. (2020). Qualification details: NWP40515 - Certificate IV in Water Industry Operations (Release 2). Retrieved from https://training.gov.au/Training/Details/NWP40515.

[9] Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. (2019). A Review of Cybersecurity Incidents in the Water Sector. Journal of Environmental Engineering. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686.

[10] Masud, U. T. (2017). Incorporating Cybersecurity into Water Utility Master Planning: A Strategic, Cost-Effective Approach to Mitigate Control System Risk. Retrieved from https://literature.rockwellautomation.com/idc/groups/literature/documents/wp/water-wp002_-en-e.pdf.

[11] Anderson, N., & Phillips, B. (2013). Water and wastewater SCADA cybersecurity: Strategic approach to water and wastewater network architecture and segmentation. InTech Magazine, Sep-Oct.

[12] Bartlett, S. & Northcott, K. (2019). The Value of Water Industry Operator Competency: The What, Why and How. WaterWorks, November, 11-14.

[13] Brumfield, C. (2020). Attempted cyberattack highlights vulnerability of global water infrastructure. Retrieved from https://www.csoonline.com/article/3541837/attempted-cyberattack-highlights-vulnerability-of-global-water-infrastructure.html.

[14] Amengor, J. (2019). Cyber Security of / for Water Utilities in Africa. Retrieved from https://iwa-network.org/cyber-security-of-for-water-utilities-in-africa/.

[15] Zoe, E. (2019). What you need to know (and do) about cybersecurity training. Retrieved from https://www.efrontlearning.com/blog/2019/03/cyber-security-training-for-employees-101.html.

[16] Brook, C. (2018). What is SCADA Security? Retrieved from https://digitalguardian.com/blog/what-scada-security.

[17] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). NIST Special Publication 800-82, Revision 2, National Institute of Standards and Technology, U.S. Department of Commerce.

[18] ELEKS Operations OU. (2019). SCADA Cyber Security Threats and Countermeasures: Ultimate Checklist. Retrieved from https://hackernoon.com/scada-cyber-security-threats-and-countermeasures-ultimate-checklist-f236f56938cd.

[19] Daalder, E. (2020). SCADA Cyber Security Information on Securing SCADA systems. Yokogawa Electric Corporation, Global SCADA Center.