The Identification of Cybersecurity Work Roles for the Water Sector in South Africa

Aby Melanie[1], Annlize Marnewick[1] and Sune von Solms[2]
[1]Postgraduate School of Engineering Management, University of Johannesburg, South Africa
[2]Department of Electrical and Electronic Engineering, University of Johannesburg, South Africa

aby.melany@gmail.com
amarnewick@uj.ac.za
svonsolms@uj.ac.za

0000-1111-2222-3333
1111-2222-3333-4444
0000-0002-1857-1683

Abstract: This paper presents the results of a content analysis conducted on the work roles of cybersecurity practitioners for the water sector of South Africa. The paper presents literature review findings on national and international frameworks and guidelines detailing cyber security considerations for the South African water sector as well as national and international guidelines and frameworks which detail the various work roles carried out by cybersecurity practitioners in an organisation. The study found that cyber security considerations and work roles such as physical security of assets, testing and assessment of cybersecurity methods, supply chains cyber security as well as incident investigation and interfacing with law enforcement, were not well defined for cyber security discipline. The study delivers a framework detailing the work roles of cybersecurity practitioners which can be applied to the South African water sector.

Keywords: Cybersecurity, work roles, water sector

1. Introduction

The water sector has attempted to bridge the gap between operating and information technologies by overlapping these systems to reduce maintenance costs and optimise the control and monitoring systems. The potential for cyber threats has increased due to the overlapping of these systems, (Wei et al., 2010; Skiba, 2020). It is important to note that critical infrastructure, such as the water infrastructure, is vulnerable if the information technology systems are not technically well protected, (Cavelty, 2007; Germano, 2019). By not having it protected, this leads to potential cyber-attacks which is detrimental to the conservation of water quality and quantity, (Stouffer and Candell, 2014; Park and Park, 2018). The resources and capabilities for detecting, preventing, and mitigating cyber risks are currently inadequate for many utilities, (Germano, 2019). To circumvent this, the National Cybersecurity Policy Framework (NCPF) was released by the South African government in 2015, however the framework does not outline the cybersecurity practitioners work roles for the water sector of South Africa (SA), (State Security Agency, 2015). This work aims to rectify this shortcoming by studying the defined work roles within the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CWF), (Petersen *et al.*, 2020), and other international and national best practice guidelines and frameworks to develop a work roles framework for cyber security practitioners in the water sector of SA. The focus of this research was on the water sector, but can be utilised in other critical infrastructure sectors as the results prove to be overarching and applicable to the wider critical infrastructure sector. To develop the framework, the study defines the water sector organisational structure from literature, the cybersecurity considerations, and based on the defined considerations, define cybersecurity work roles and close any gaps identified. The development of this framework will assist in detection, mitigation and prevention of future cyber threats.

2. Literature Review

2.1 Water sector organisational structure

To start to address the concerns around the threat to water quantity and quality, the South African water sector organistional structure needed to be understood. Legislation and policies is developed at the ministerial level, (Beck *et al.*, 2016). Departmental level is responsible for governance related to policies and legislation. This level also ensures and enforces compliance, (Ruiters and Matji, 2015). National and regional levels is responsible for the development and management of all procedures, (GreenCape, 2014). Local level is responsible to ensure

that policies and procedures are carried out within their jurisdictions. Plant level carries out and implements all procedure and policies. This level will also monitor, control and report any anomalies which may adversely impact plant operations, (GreenCape, 2014; Ruiters and Matji, 2015; Beck *et al.*, 2016).

2.2 Frameworks and guidelines to define the cybersecurity considerations for the water sector

Internationally, a variety of cybersecurity frameworks, guidelines and standards have been produced or are in the process of being developed, (Panguluri, Phillips and Cusimano, 2011; Germano, 2019). The International Organisation of Standards (ISO) 27002 has been adopted by South African Bureau of Standards (SABS) which specifies an organisation's minimum information security criteria, (International Organisation for Standardisation, 2013). Other data sources identified includes:

- Guide to Industrial Control Systems (ICS) Security, (Stouffer et al., 2015),
- 15 cybersecurity fundamentals for water and wastewater utilities: Best practices to reduce exploitable weaknesses and attacks, (Water Information Sharing and Analysis Center, 2019)
- American Water Works Association (AWWA) Water sector cybersecurity risk management guidance, (Yost, 2019)
- Roadmap to secure control systems in the water sector, (Water Sector Coordinating Council Cyber Security Working Group, 2008).

The documents mentioned can be used to define the cyber security considerations for the water sector of South Africa.

Gaps identified from literature indicates that the cyber security industry is relatively new and many of its standards and guidelines are still in development, (Panguluri *et al.*, 2011). Not all the cyber security requirements for the water sector have been identified but rather has been developed based on known threats and vulnerabilities, (Water Sector Coordinating Council Cyber Security Working Group, 2008; Germano, 2019; Yost, 2019). Literature also indicates that methods of physical security, access and authentication, software enhancements and privacy enhancements are all cyber security components which are lacking. Another gap identified is the requirements for improving the security between the business and ICS network as well as intrusion detection, (Panguluri *et al.*, 2011; Clark *et al.*, 2016; Germano, 2019).

2.3 Frameworks and guidelines to define the work roles of cybersecurity practitioners

Skills Framework for the Information Age (SFIA) is a model for characterising and managing skills and competencies for Information and Communication Technologies (ICT) and cyber security professionals. The model assists with understanding IT skills in general and it contains security-related skills, (Furnell, 2021). SFIA describes the abilities and competencies required by professionals in positions involving information and communication technology and cyber security, (SFIA Foundation, 2018).

According to Caulkins, Marlowe and Reardon, (2019), the demand for cyber security practitioners is growing. Competent cybersecurity practitioners are hard to come by in all industries and companies, (Campbell, O'Rourke and Bunting, 2015). The NIST NICE CWF acts as a guiding principle for the development of a unified cyber security workforce. The NIST NICE CWF details the requirements for work force identification, standardises development of work role descriptions, qualification requirements and training requirements for the development of a capable and ready workforce, (Dawson, Taveras and Taylor, 2019; Schmeelk and Dragos, 2020). The NIST NICE CWF was released in order to develop a process for determining specific cybersecurity work roles (Campbell *et al.*, 2015). The NIST NICE CWF was used as the baseline data source for the study.

Gaps identified shows that the educational programs at various institutes are not aligned to the NIST NICE CWF, especially in the Analyse and Investigate categories, (Caulkins *et al.*, 2019; Saharinen, Backlund and Nevala, 2020). Another gap is that the NIST NICE CWF focusses on the technical skills required for the cyber security work force however, research, (Campbell *et al.*, 2015; Caulkins *et al.*, 2019), indicates that non-technical skills are just as important as that of the technical kind. Based on the current professionals within the industry, the work roles framework that was identified may not be implementable due to the lack of educational programs available, grasp of non-technical skills and the availability of experienced individuals.

3. Methodology

This study adopted the qualitative content analysis methodology using secondary data identified from literature. This methodology is utilised because it assures that the original data is preserved, the data is analysed systematically rather than selectively, and it is used to analyse qualitative data and construct frameworks, (Lancaster, 2005; Sekaran and Bougie, 2016). Firstly, the cybersecurity considerations for the water sector were defined by using the ISO 27002 as the baseline data source. Verification and validation of the considerations extracted from ISO 27002 was performed by using the other data sources identified in section 2.2. Secondly, the work roles for cyber security practitioners were defined by listing all the cyber security work roles and their definitions from the NIST NICE CWF. A meaning unit was defined, in the case of this research, defining the meaning unit refers to condensing of the work roles definition. The meaning unit was then categorised and coded. The code was used to match the work role to a specific cyber security consideration. Validation and verification were carried out by using SFIA. The results from the data analysis process were interpreted to construct a framework to address the research aim.

4. Results, Analysis and Discussions

4.1 Water sector cybersecurity considerations

To establish the appropriate work roles for cybersecurity practitioner in the water sector, the cybersecurity considerations for the South African water sector was firstly determined. The considerations were collected from four (4) different data sources, as shown in sections 2.2. The data collected was combined and examined to create a comprehensive set of cybersecurity consideration for the water sector in SA. Firstly, ISO 27002, was used to list and define the baseline of cybersecurity considerations. Secondly, these cybersecurity considerations were verified against the three (3) other data sources. They were verified by performing latent and manifest analysis on the definitions of the considerations. A total of fourteen (14) considerations was defined.

4.2 Cybersecurity practitioners work roles for the South African water sector

Data was collected from the NIST NICE CWF and analysed to define the work roles of cyber security practitioners in the water sector based on cyber security considerations defined in section 4.1. SFIA was used for verification and validation. **Fig. 1** shows the steps that were followed to develop a comprehensive set of cyber security practitioner work roles for the water sector in SA.

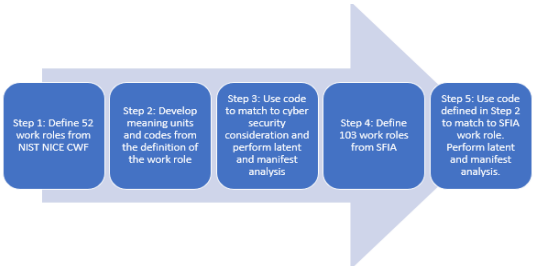

Fig. 1. Steps followed to develop a comprehensive set of cyber security practitioner work roles for the water sector in SA.

Fig. 2 illustrates how steps 1-3 was applied to the data analysis process by using the work role *Risk Management RSK: Authorising Official* from the NIST NICE CWF.

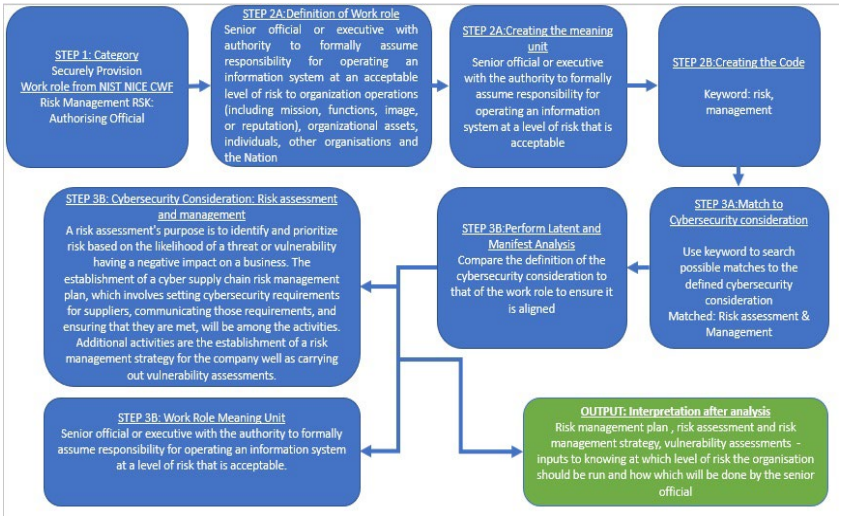

Fig. 2. Implementation of step 1-3 on one work role identified from NIST NICE CWF

Fig. 3 illustrates the application of the verification and validations steps 4- 5 on the work role, *Risk Management RSK: Authorising Official* from the NIST NICE CWF.

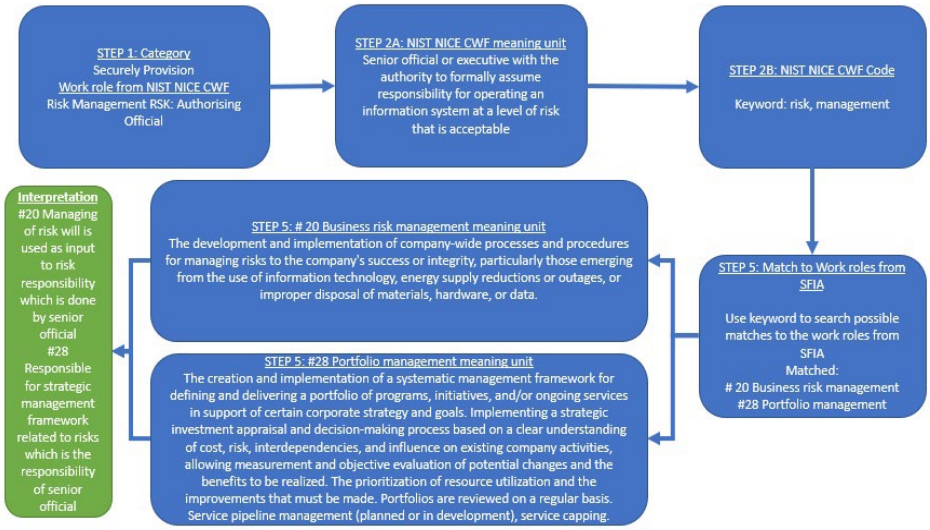

Fig. 3. Implementation of steps 4-5 on one work roles identified form NIST NICE CWF

Table 1 shows the summary of the results of the data analysis process for the NIST NICE CWF Work role: *Risk management RSK: Authorising Official*. The work role matched the cyber security consideration *Risk Assessment & Management*. It was also verified and validated by matching to the SFIA work roles *Business Manager* and *Portfolio Manager*. This will be added to the construction of the work roles framework.

Table 1. Results for the Risk management RSK: Authorising Official

Category	NIST NICE CWF Work role	Cyber Security Consideration	SFIA Work role
Securely Provision	Risk Management RSK: Authorising Official	Risk assessment and management	1. Business risk manager 2. Portfolio manager

By following the steps in **Fig. 1**, a list of thirty-seven (37) work roles was identified. Additionally, six (6) gaps have also been identified. Four (4) gaps were related the cyber security considerations and two (2) gaps was related to the defined work roles within the NIST NICE CWF.

4.3 Gaps identified

Two types of gaps have been identified. The first set of gaps were related to the water sector cybersecurity considerations. No considerations match the following work roles namely, 1. *Test & Evaluation: System Test & Evaluation Specialist*, 2. *Cyber Investigation: Cyber Crime Investigator*, 3. *Digital Forensics: Law Enforcement/Counterintelligence Forensics Analyst* and 4. *Digital Forensics: Cyber Defence Forensics Analyst.* The second set of gaps were related to the NICE NIST CWF work role. The work roles did not match the following cyber security considerations: 1. *Physical & Environmental Security* and 2. *Securing the Supply Chain*. The gaps related to the cybersecurity considerations revealed that little emphasis is currently upon identifying where the cyber threats emanate from, as well as apprehension of the perpetrators. This is a very important aspect to consider as this will influence consequences applied to cyber attackers and future cyber-criminal activity. Gaps related to the defined work roles indicate that third party cyber-attacks are currently not considered as a high risk. Cyber-attacks can come from any source and may have devastating impacts on an organisation. Another gap identified was related to physical security of cybersecurity assets. Hardware can easily be infiltrated by a cyber attacker. To close the gap related to the cybersecurity consideration and the defined work roles from NIST NICE CWF, the following was done:

- The definitions of the required consideration was adapted from the definition of the work role identified as well as the definition from SFIA.
- The methodology of creating new work roles was applied by defining the task by adapting a definition from SFIA and the cybersecurity considerations.

4.4 Framework for cybersecurity practitioners for the South African water sector

The results from the data analysis process were used to develop a framework for cyber security practitioners which defines the cyber security work roles for the water sector of SA. The gaps identified was addressed and new work roles and cybers security considerations were defined. The now complete list of work roles and cyber security considerations were matched to the levels within the water sector organisation structure which was defined from literature.

Table 2. Cyber security work roles for the water sector of SA Framework

Cyber security considerations	Work Role	Organisation structure
Governance	Executive Cyber Leadership: Executive Cyber Leadership	Ministerial
	Strategic Planning and Policy: Cyber Policy and Strategy Planner	Departmental
Human Resource Security & Cyber security Awareness	Strategic Planning and Policy: Cyber Workforce Developer and Manager	Departmental
Compliance	Legal Advice and Advocacy: Cyber Legal Advisor	National & Regional
	Legal Advice and Advocacy: Privacy Officer/Privacy Compliance Manager	National & Regional
Risk assessment & Management	Risk Management (RSK): Authorising Official	National & Regional
Governance	Conducts evaluations of an IT program or its individual components, to determine compliance with published standards	Local
Business Continuity, incidents, emergencies and Disaster Recovery planning	Cyber Operational Planning: Cyber Intel Planner	Local
	Cyber Operational Planning: Cyber Ops Planner	Local
Cryptography, Design and implementation of improved security systems	Systems Development: Systems Developer	Local
	Systems Architecture: Security Architect	Local
Participate in Partnership and Outreach for information sharing and collaboration	Cyber Operational Planning: Partner Integration Planner	Local
	Cyber Defence Infrastructure Support: Cyber Defence Infrastructure Support Specialist	Local
Human Resource Security & Cyber security Awareness	Training, Education and Awareness: Cyber Instructional Curriculum Developer	Local
	Training, Education and Awareness: Cyber Instructor	Local
Forensic analysis and law enforcement liaison for cyber crimes	Digital Forensics: Law Enforcement/Counterintelligence Forensics Analyst	Local
	Digital Forensics: Cyber Defence Forensics Analyst	Local
Governance	Cyber Security Management: Information Systems Security Manager	Works

Cyber security considerations	Work Role	Organisation structure
Business Continuity, incidents, emergencies and Disaster Recovery planning	Incident Response: Cyber Defense Incident Responder	Works
Risk assessment & Management	Risk Management (RSK): Security Control Assessor	Works
Cryptography, Design and implementation of improved security systems	Software Development: Software Developer	Works
	Software Development: Secure Software Assessor	Works
Participate in Partnership and Outreach for information sharing and collaboration	Technology R&D: Research and Development Specialist	Works
Cyber security Testing & Evaluation	Test & Evaluation: System Test & Evaluation Specialist	Works
Cryptography, Design and implementation of improved security systems	Systems Development: Information Systems Security Developer	Works
Asset Management	Data Administration: Database Administrator	Works
	Data Administration: Data Analyst	Works
	Knowledge Management: Knowledge Manager	Works
Access Control	Systems Analysis: Systems Security Analyst	Works
Communication Security	Cyber Security Management: Communications Security Manager	Works
Operations Security	Cyber Defence Analysis: Cyber Defence Analyst	Works
Systems acquisition, development and maintenance	Vulnerability Assessment and Management: Vulnerability Assessment Analyst	Works
	Warning/Threat Analysis: Threat/Warning Analyst	Works
	Exploitation Analysis: Exploitation Analyst	Works
	All-Source Analysis: All-Source Analyst	Works
	All-Source Analysis: Mission Assessment Specialist	Works
	Targets: Target Developer	Works
	Targets: Target Network Analyst	Works
	Language Analysis: Multi-Disciplined Language Analyst	Works
Operations Security	Cyber Operations: Cyber Operator	Works
Investigation of cyber crimes	Cyber Investigation: Cyber Crime Investigator	Works
Physical & Environmental Security	Security Officer	Works
Securing the Supply Chain	Third Party Cyber Security Officer	Works

Table 2, shows all Forty-three (43) work roles which have been defined to a level within the water sector's organisational structure. It should be noted that the framework indicates the minimum work roles required based on the water sector organisational structure developed from literature.

5. Recommendations and Conclusion

The work roles defined for cyber security practitioners should be filled by the organisation to ensure that prevention, mitigation and detection of cyber threats occur to reduce this emerging risk. The water sector needs to start sharing experiences of cyber threats and events across sectors as this will assist in implementing lessons learnt and possibly preventing future incidents. Application of the framework needs to start at ministerial level where legislation must be developed, reviewed and implemented and a clear plan for implementation is also developed. Departmental level of the water sector ensures that the legislation, policies and procedures are governed and enforced by measuring compliance. This level must also ensure that resources is made available to carry out the required cyber security practitioner work roles. National and regional levels of the water sector must ensure the development of procedures and management of thereof. Local level must ensure that policies and procedures are carried out correctly within their jurisdiction. Plant level must ensure that legislation, policies and procedure are carried out. The findings of this study should be used to identify existing resources to meet the cyber security workforce needs. Secondly, an assessment of the educational programs needs to be done to ensure alignment to the required work roles for the sector.

References

Beck, T., Rodina, L., Luker, E. and Harris, L. (2016) *Institutional and Policy Mapping of the water sector in South Africa*. Cape Town. doi: 10.13140/RG.2.2.32761.88164.

Campbell, S. G., O'Rourke, P. and Bunting, M. F. (2015) 'Identifying dimensions of cyber aptitude: The design of the cyber aptitude and talent assessment', *Proceedings of the Human Factors and Ergonomics Society*, 2015-Janua, pp. 721–725. doi: 10.1177/1541931215591170.

Caulkins, B., Marlowe, T. and Reardon, A. (2019) 'Cybersecurity Skills to Address Today's Threats', *Advances in Intelligent Systems and Computing*, 782, pp. 187–192. doi: 10.1007/978-3-319-94782-2_18.

Cavelty, M. D. (2007) *Critical information infrastructure_ vulnerabilities, threats and responses*. 1st edn, *ICTs and International Security*. 1st edn. Zurich, Switzerland.

Clark, R. M., Panguluri, S., Nelson, T. D. and Wyman, R. P. (2016) *Protecting Drinking Water Utilities from Cyber Threats*. Idaho.

Dawson, M., Taveras, P. and Taylor, D. (2019) 'Applying Software Assurance and Cybersecurity NICE Job Tasks through Secure Software Engineering Labs', *Procedia Computer Science*, 164, pp. 301–312. doi: 10.1016/j.procs.2019.12.187.

Furnell, S. (2021) 'The cybersecurity workforce and skills', *Computers and Security*, 100, p. 102080. doi: 10.1016/j.cose.2020.102080.

Germano, J. H. (2019) *Cybersecurity Risk & Responsibility in the Water Sector*. New York.

GreenCape (2014) *Market Intelligence Report: Water*. Cape Town.

International Organisation for Standardisation (2013) *ISO/IEC 27002:2013 Information Technology- Security techniques - Code of practice for information security controls*. ISO/IEC.

Lancaster, G. (2005) *Research Methods in Management: A Concise introduction to research in management and business consultancy*. Burlington, MA: Elsevier Butterworth-Heinemann.

Panguluri, S., Phillips, W. and Cusimano, J. (2011) 'Protecting water and wastewater infrastructure from cyber attacks', *Frontiers of Earth Science*, 5(4), pp. 406–413. doi: 10.1007/s11707-011-0199-5.

Park, S.-N. and Park, D.-W. (2018) 'Cybersecurity System for Water Treatment SCADA System', *Journal of Engineering and Applied Sciences*, 13(11), pp. 8712–8715. Available at: http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf.

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A. and Witte, G. (2020) *Workforce Framework for Cybersecurity (NICE Framework)*. Gaithersburg, MD. doi: 10.6028/NIST.SP.800-181r1.

Ruiters, C. and Matji, M. P. (2015) 'Water institutions and governance models for the funding, financing and management of water infrastructure in South Africa', *Water SA*, 41(5), pp. 660–676. doi: 10.4314/wsa.v41i5.09.

Saharinen, K., Backlund, J. and Nevala, J. (2020) 'Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework', *ACM International Conference Proceeding Series*, pp. 172–176. doi: 10.1145/3436756.3437041.

Schmeelk, S. and Dragos, D. (2020) 'Wireless Security: Examining the next NICE Framework Iteration based on Industry Requirements', *Cybersecurity Skills Journal: Practice and Research*, (Special), pp. 59–73.

Sekaran, U. and Bougie, R. (2016) *Research Methods for Business: A skills building approach*. Seventh Ed. John Wiley & Sons Ltd.

SFIA Foundation (2018) *Skills Framework of the Information Age (SFIA): The complete reference*. England. Available at: https://www.sfia-online.org/en.

Skiba, R. (2020) 'Water Industry Cyber Security Human Resources and Training Needs', *International Journal of Engineering Management*, 4(1), p. 11. doi: 10.11648/j.ijem.20200401.12.

State Security Agency (2015) *The National Cybersecurity Policy Framework for South Africa*. Available at: www.gpwonline.co.za.

Stouffer, K. and Candell, R. (2014) 'Measuring impact of cybersecurity: On the performance of industrial control systems', *Mechanical Engineering*, 136(12), pp. 4–7. doi: 10.1115/1.2014-dec-5.

Water Information Sharing and Analysis Center (2019) *15 Cybersecurity Fundamentals for Water and Wastewater Utilities: Best practices to reduce exploitable weaknesses and attacks*. Washington. Available at: www.waterisac.org.

Water Sector Coordinating Council Cyber Security Working Group (2008) *Roadmap Secure Control Systems in the water sector*, *Control*. Washington DC.

Wei, D., Lu, Y., Jafari, M., Skare, P. and Rohde, K. (2010) 'An integrated security system of protecting smart grid against cyber attacks', in *Innovative Smart Grid Technologies Conference, ISGT 2010*. doi: 10.1109/ISGT.2010.5434767.

Yost, W. (2019) *Water Sector Cybersecurity Risk Management Guidance*.