# WILEY

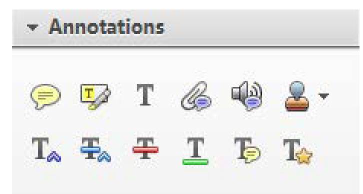
**Online Proofing System Instructions**

The Wiley Online Proofing System allows proof reviewers to review PDF proofs, mark corrections, respond to queries, upload replacement figures, and submit changes directly from the locally saved PDF proof.

**1.** For the best experience when reviewing your PDF proof ensure you are connected to the internet. This will allow the locally saved PDF proof to connect to the central Wiley Online Proofing System server. If you are connected to the Wiley Online Proofing System server you should see a green check mark icon above in the yellow banner.

Connected Disconnected

**2.** Please review the article proof on the following pages and mark any corrections, changes, and query responses using the Annotation Tools outlined on the next 2 pages.




**3.** Save your proof corrections by clicking the "Publish Comments" button in the yellow banner above. Corrections don't have to be marked in one sitting. You can publish comments and log back in at a later time to add and publish more comments before you click the "Complete Proof Review" button below.


**4.** If you need to supply additional or replacement files <u>bigger</u> than 5 Megabytes (MB) do not attach them directly to the PDF Proof, please click the "Upload Files" button to upload files:

Upload files

Click Here

**5.** When your proof review is complete and all corrections have been published to the server by clicking the "Publish Comments" button, please click the "Complete Proof Review" button below:

**IMPORTANT:** Did you reply to all author queries found on the first page of your proof?

**IMPORTANT:** Did you click the "Publish Comments" button to save all your corrections? Any unpublished comments will be lost.

**IMPORTANT:** Once you click "Complete Proof Review" you will not be able to add or publish additional corrections.

Complete Proof Review

Click Here

# WILEY

## Online Proofing System

### Enabling the Adobe PDF Viewer

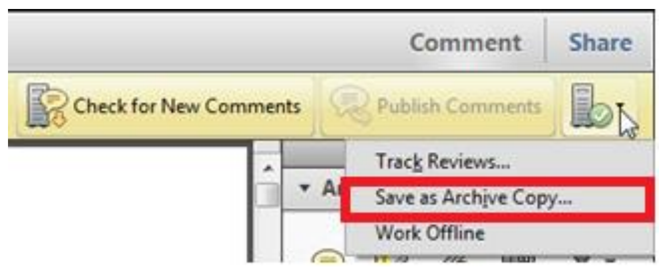
In order to proof your article Adobe Reader or Adobe Acrobat needs to be your browser's default PDF viewer. See how to set this up for Internet Explorer, Firefox, and Safari at [https://helpx.adobe.com/acrobat/using/display-pdf-in-browser.html](https://helpx.adobe.com/acrobat/using/display-pdf-in-browser.html)

Google Chrome and Microsoft Edge do not support Adobe Reader or Adobe Acrobat as a PDF Viewer. We recommend using Internet Explorer, Firefox, or Safari.

**1.** Mark your corrections, changes, and query responses using the Annotation Tools outlined on the next 2 pages.

**2.** Save your proof corrections by clicking the “Publish Comments” button in the yellow banner above. Corrections don’t have to be marked in one sitting. You can publish comments and log back in at a later time to add and publish more comments before you click the “Complete Proof Review” button.


**3.** When your proof review is complete we recommend you download a copy of your annotated proof for reference in any future correspondence concerning the article before publication. You can do this by clicking on the icon to the right of the ‘Publish Comments’ button and selecting ‘Save as Archive Copy…’.




**IMPORTANT:** Did you reply to all queries listed on the Author Query Form appearing before your proof?

**IMPORTANT:** Did you click the “Publish Comments” button to save all your corrections? Any unpublished comments will be lost.

**IMPORTANT:** Once you click “Complete Proof Review” you will not be able to add or publish additional corrections.

**4.** When your proof review is complete and all corrections have been published to the server by clicking the “Publish Comments” button, please click the “Complete Proof Review” button appearing above the proof in your web browser window.

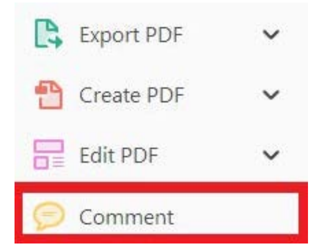
WILEY

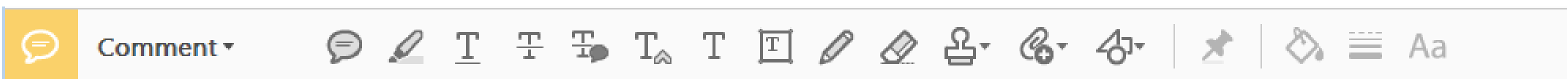
## USING e-ANNOTATION TOOLS FOR ELECTRONIC PROOF CORRECTION

**Required software to e-Annotate PDFs: Adobe Acrobat Professional or Adobe Reader (version 11 or above). (Note that this document uses screenshots from Adobe Reader DC.)**
**The latest version of Acrobat Reader can be downloaded for free at: http://get.adobe.com/reader/**

Once you have Acrobat Reader open on your computer, click on the Comment tab (right-hand panel or under the Tools menu).

This will open up a ribbon panel at the top of the document. Using a tool will place a comment in the right-hand panel. The tools you will use for annotating your proof are shown below:



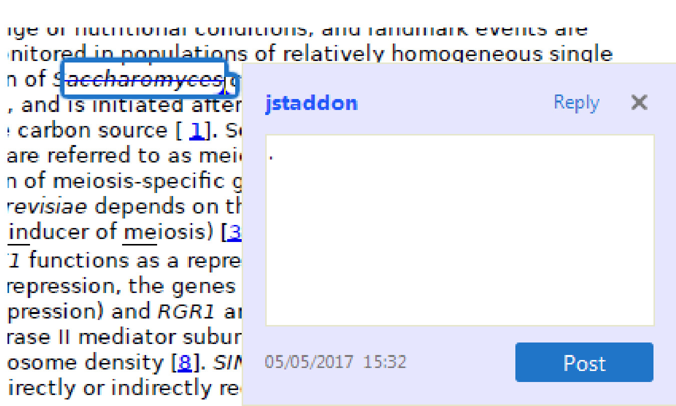




### 1. Replace (Ins) Tool – for replacing text.

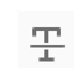
Strikes a line through text and opens up a text box where replacement text can be entered.

**How to use it:**

- Highlight a word or sentence.
- Click on .
- Type the replacement text into the blue box that appears.



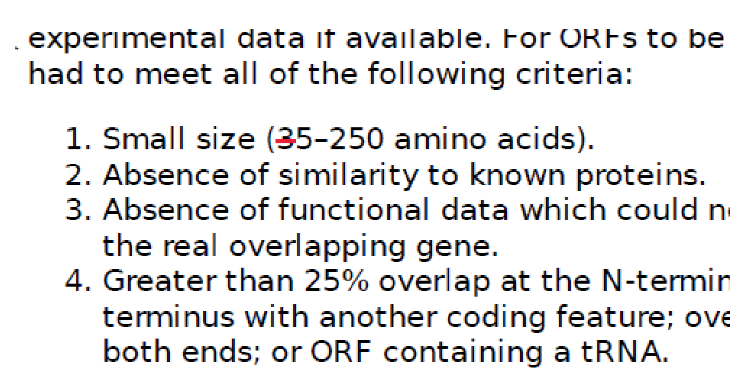

### 2. Strikethrough (Del) Tool – for deleting text.



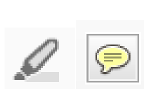
Strikes a red line through text that is to be deleted.

**How to use it:**

- Highlight a word or sentence.
- Click on ..
- The text will be struck out in red.



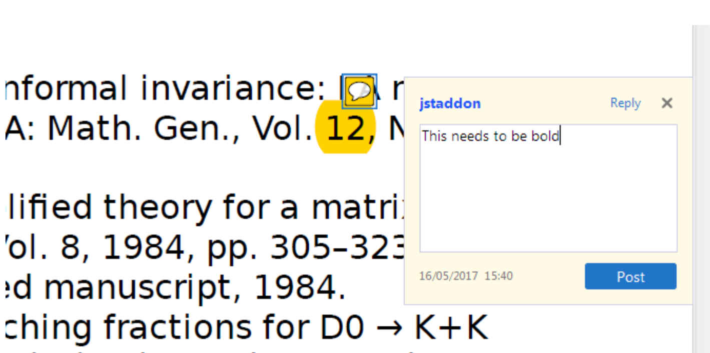

### 3. Commenting Tool – for highlighting a section to be changed to bold or italic or for general comments.



Use these 2 tools to highlight the text where a comment is then made.

**How to use it:**

- Click on .
- Click and drag over the text you need to highlight for the comment you will add.
- Click on .
- Click close to the text you just highlighted.
- Type any instructions regarding the text to be altered into the box that appears.

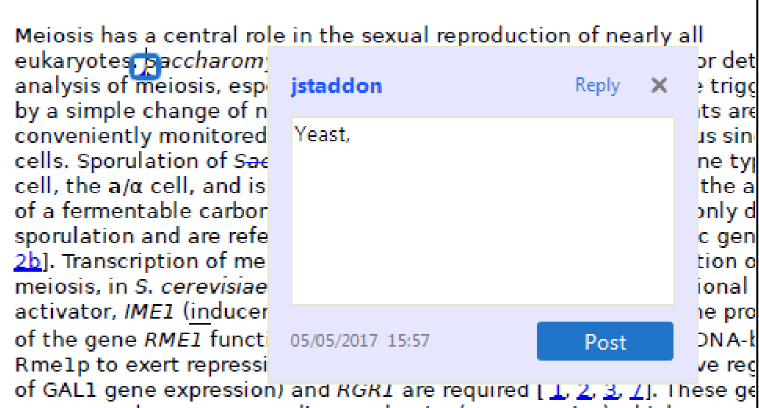



### 4. Insert Tool – for inserting missing text at specific points in the text.

Marks an insertion point in the text and opens up a text box where comments can be entered.

**How to use it:**

- Click on .
- Click at the point in the proof where the comment should be inserted.
- Type the comment into the box that appears.



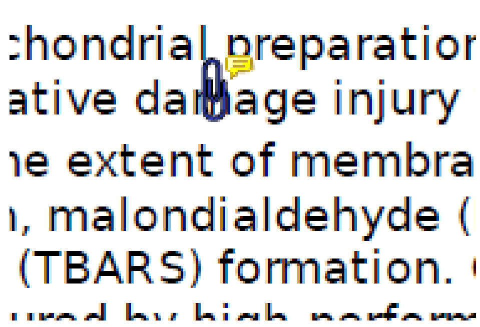
**5. Attach File Tool – for inserting large amounts of text or replacement figures.**

Inserts an icon linking to the attached file in the appropriate place in the text.

**How to use it:**

- Click on .
- Click on the proof to where you'd like the attached file to be linked.
- Select the file to be attached from your computer or network.
- Select the colour and type of icon that will appear in the proof. Click OK.

  The attachment appears in the right-hand panel.

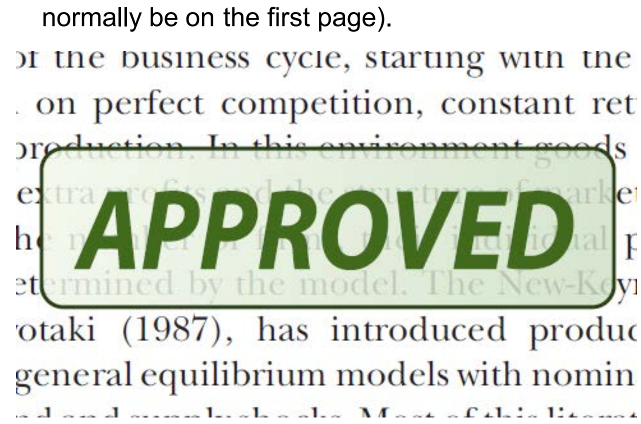



**6. Add stamp Tool – for approving a proof if no corrections are required.**

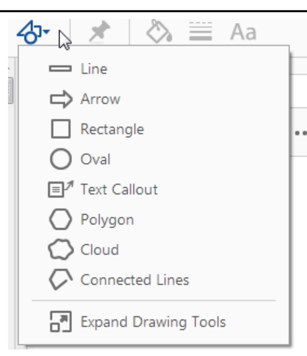
Inserts a selected stamp onto an appropriate place in the proof.

**How to use it:**

- Click on .
- Select the stamp you want to use. (The Approved stamp is usually available directly in the menu that appears. Others are shown under *Dynamic*, *Sign Here*, *Standard Business*).
- Fill in any details and then click on the proof where you'd like the stamp to appear. (Where a proof is to be approved as it is, this would normally be on the first page).




Drawing tools available on comment ribbon

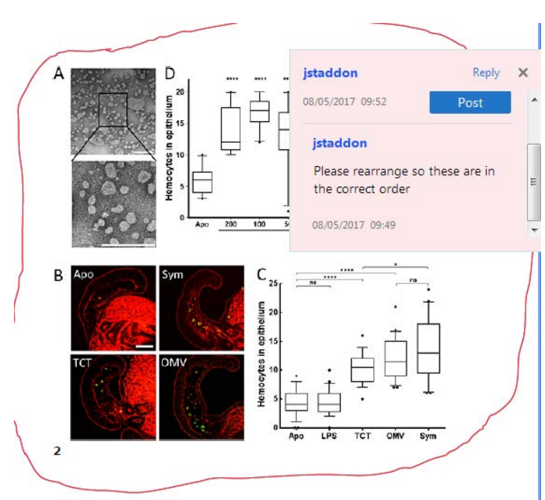



**7. Drawing Markups Tools – for drawing shapes, lines, and freeform annotations on proofs and commenting on these marks.**

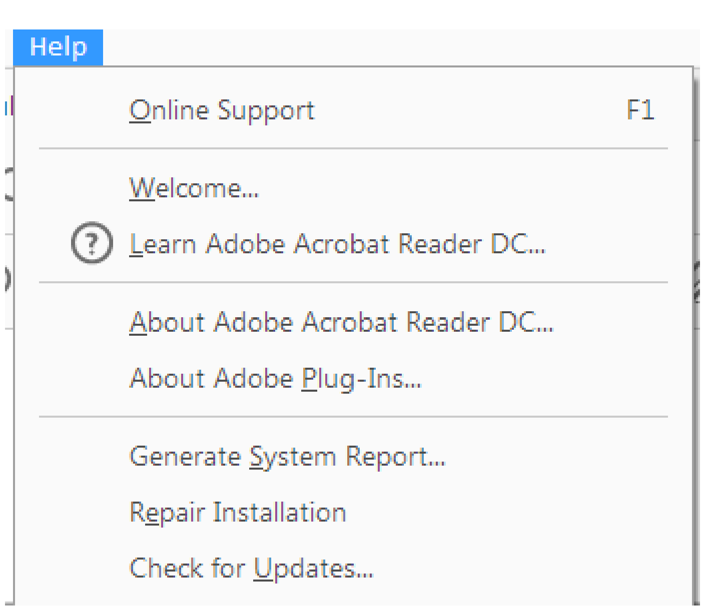
Allows shapes, lines, and freeform annotations to be drawn on proofs and for comments to be made on these marks.

**How to use it:**

- Click on one of the shapes in the Drawing Markups section.
- Click on the proof at the relevant point and draw the selected shape with the cursor.
- To add a comment to the drawn shape, right-click on shape and select *Open Pop-up Note*.
- Type any text in the red box that appears.




**For further information on how to annotate proofs, click on the Help menu to reveal a list of further options:**



WILEY

# Author Query Form

Journal: WEJ

Article: 12340

Dear Author,

During the copyediting of your manuscript the following queries arose.

Please refer to the query reference callout numbers in the page proofs and respond to each by marking the necessary comments using the PDF annotation tools.

Please remember illegible or unclear comments and corrections may delay publication.

Many thanks for your assistance.

| Query References | Query | Remarks? |
|---|---|---|
| AQ1 | AUTHOR: Please check whether the short title is OK as given. | |
| AQ2 | AUTHOR: Please confirm that the affiliations are OK as typeset. | |
| AQ3 | AUTHOR: Please confirm whether the keywords inserted from pdf is OK as typeset. | |
| AQ4 | AUTHOR: Please note that the abbreviations section has been deleted as they were detailed in the text. Please confirm whether this is OK. | |
| AQ5 | AUTHOR: Please check the phrase "increase of 782%" for clarity. | |
| AQ6 | AUTHOR: "Conclusions" should be set as numbered points as per journal style. Please confirm. | |
| AQ7 | AUTHOR: Please confirm whether the following references "AWWA (2014), AWWA (2015), Clapper (2012), Fisher (2014), HSPD–7 (2002), Lipton et al. (2016), Russian Hackers (2016), Stack 8 (2015), and NGA (2015)." are OK as typeset. | |
| AQ8 | AUTHOR: There is no mention of National Institute of Standards and Technology (NIST) (2014) in the text. Please provide citation for the same. | |
| AQ9 | AUTHOR: Please provide complete details for reference "Ponemon Institute LLC. (2013)". | |
| AQ10 | AUTHOR: Please confirm that given names (red) and surnames/family names (green) have been identified correctly. | |

# Funding Info Query Form

Please confirm that the funding sponsor list below was correctly extracted from your article: that it includes all funders and that the text has been matched to the correct FundRef Registry organization names. If a name was not found in the FundRef registry, it may be not the canonical name form or it may be a program name rather than an organization name, or it may be an organization not yet included in FundRef Registry. If you know of another name form or a parent organization name for a "not found" item on this list below, please share that information.

| FundRef name | FundRef Organization Name |
|---|---|
| Idaho National Laboratory | ~~[NOT FOUND IN FUNDREF REGISTRY]~~ |

J_ID: **WEJ** Customer A_ID: **WEJ12340** Cadmus Art: **WEJ12340** Ed. Ref. No.: **WEJ-8261-17.R1** Date: **31-January-18** Stage: Page: **1**

Water and Environment Journal
Promoting Sustainable Solutions
CIWEM

Water and Environment Journal. Print ISSN 1747-6585

# Protecting water and wastewater utilities from cyber-physical threats

AQ10 Robert M. Clark[1], Simon Hakim[2] & Srinivas Panguluri[3]

[1]Environmental Engineering and Public Health Consultant, Cincinnati, OH, USA; [2]Professor of Economics, and Director of the Center for Competitive
AQ2 Government at the Fox School, Temple University, Philadelphia, PA, USA; and [3]CB&I Federal Services LLC, Cincinnati, OH, USA

**Keywords**
drinking water; environmental assessment; wastewater treatment; water quality; water
AQ3 supply.

**Correspondence**
R. M. Clark, Environmental Engineering and Public Health Consultant, 9627 Lansford Drive, Cincinnati, OH 45242, USA.
Email: rmclark@fuse.net

doi:10.1111/wej.12340

## Abstract

Recent events have highlighted the need to address cybersecurity threats to systems supporting critical infrastructure and federal information systems are evolving and growing. These threats have become ubiquitous in the United States, and throughout the world. Many information and communications technology (ICT) devices and other components are interdependent so that disruption of one component may have a negative, cascading effect on others. In the United States, the Federal role in cyber-security has been debated for more than a decade but creating a policy is complicated because in the United States, State and local governments are the major institutions responsible for providing services to their populations. It is that critical infrastructure such as Publically Owned Treatment Works (POTWs) and Public Water Systems (PWSs) adopt suitable countermeasures to prevent or minimise the consequences of cyber-attacks. This paper discusses both technological and procedural techniques that can be used to protect against cyber-threats.



AQ4

## Introduction

In a recent issue of the New York Times, David Lipton and his colleagues reported that Russian Intelligence had 'hacked' the Democratic National Committee in an attempt to influence the US Presidential Election (Lipton *et al*. 2016). Clearly, challenges related to cyber-security have the potential for becoming one of the most significant issues in the 21st century. In 2009, Barack Obama, President of the United States (US) declared cyber threats to be among 'the most serious economic and national security challenges we face as a nation' and stated that 'America's economic prosperity in the 21st century will depend on cyber-security (Obama 2009)'. In January 2012, the US Director of National Intelligence testified before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives that cyber threats pose a critical national and economic security concern (Clapper 2012). To further highlight the importance of these threats, on October 11, 2012, the US Secretary of Defense stated that the collective result of attacks on our nation's critical infrastructure (CI) could be 'a cyber-Pearl Harbor; an attack that would cause physical destruction and the loss of life (Panetta 2012)'. According to a 2013 report issued by the US General Accountability Office (GAO), cybersecurity threats to systems supporting CI and federal information systems are evolving and growing (US GAO 2013). In addition, the US GAO conducted a number of other studies attempting to highlight and document US vulnerability to cyber-threats. These concerns apply to governments throughout the world.

A critical aspect of cybersecurity is the need to protect CI. In an attempt to enhance and improve the security and resiliency of US CI through voluntary, and collaborative efforts, in February 2013, the US President issued Executive Order 13636 (Fischer *et al*. 2013). The order expanded an existing Department of Homeland Security (DHS) program for information; sharing and collaboration between the government and the private sector by:

- Developing a process for identifying CI that have a high priority for protection;
- Requiring the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework of standards and best practices for protecting CI; and
- Requiring regulatory agencies to determine the adequacy of current requirements and their authority to establish requirements to address the risks.

Cyber-threats to US infrastructure, and other assets, are of growing concern to policymakers. These threats have become ubiquitous in the United States and are troublesome because many information and communications technology (ICT) devices and other components are interdependent. Therefore, disruption of one component may have a negative, cascading effect on others. Cyber-attacks might include denial of service, theft or manipulation of data. Damage to CI through a cyber-attack could have a significant impact on national security, the economy, and the livelihood and safety of citizens. It is clear that cyber-security issues include not only the threats associated with information technology but also involve physical threats to CI.

Even though cyber-threats pose a major threat to CI, in the United States, the Federal role in cyber-security has been debated for more than a decade. Action at the Federal level for protecting CI is limited because of the political structure of the United States. In the United States, State and local governments have been the major institutions responsible for providing services to their populations. However, the US Constitution provides for a separation of powers between the States and the Federal government. In order to bridge this gap, the National Governors Association (NGA 2015), a non-partisan organisation representing the interests of the fifty states and trust territories, has begun taking action in this important area (NGA 2015). Governments in countries that do not have the political separation of power that exists in the United States, may therefore be able to adopt a more integrated approach to cyber-security (Tabansky 2016).

From a public health and an economic perspective, public water supply (PWS) and wastewater systems represent a CI that needs protection. After September 11, 2001, the federal government directed efforts to secure the nation's CI and initiated programs such as the National Strategy to Secure Cyberspace (Bush 2003). This program addresses the vulnerabilities of Supervisory Control and Data Acquisition (SCADA) systems and Information Control Systems (ICSs) and calls for the public and private sectors to work together to foster trusted control systems (Dakin *et al*. 2009; Edwards 2010). This paper discusses the vulnerability of water supply and wastewater to cyber-threats and suggests actions for dealing with these threats.

## Cyber-security challenges in the United States

The US GAO has conducted a number of comprehensive studies on the vulnerability of US governmental and societal functions to cyber-threats. According to these studies advanced persistent threats (APTs) pose increasing risks in the United States and throughout the world (US GAO 2011). APTs occur where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives repeatedly over an extended period of time. Some of these adversaries may be foreign militaries or organized international crime. Growing and evolving threats can potentially affect all segments of society, including individuals, private businesses, government agencies and other entities.

National threats to security include those aimed against governmental systems and networks including military systems, as well as against private companies that support government activities or control CI (US GAO 2011). Cyber-threats may target commerce and intellectual property. These threats may include obtaining confidential intellectual property of private companies and governments, or individuals with the objective of using that intellectual property for economic gain. Threats to individuals could lead to the unauthorised disclosure of personally identifiable information, such as taxpayer data, Social Security numbers, credit and debit card information or medical records. The disclosure of such information could cause harm to individuals, including identity theft, financial loss and embarrassment.

Cyber-attacks can result in the loss of sensitive information and damage to economic and national security, the loss of privacy, identity theft or the compromise of proprietary information or intellectual property. According to the US Computer Emergency Readiness Team (US-CERT), over this period, the incidents have increased from 5 503 to 48 562; an increase of 782% (US GAO 2013). AQ5

The following examples illustrate the potential for attacking CI in the United States:

- In Eastern Ukraine in late December, 2015 power was cut to more than 600 000 homes and Russia was identified as the likely source of the attack. Ukraine's security service and the Ukraine government blamed Russia for the attack. The US including experts at the CIA, National Security Agency and the DHS are investigating whether samples of malware recovered from the company's network indicate that the blackout was caused by hacking and whether it can be traced back to Russia. Researchers from a private global security company claimed they had samples of the malicious code that affected three of the region's power companies, causing 'destructive events'. The group behind the attack has been identified as the 'the Sandworm gang', which is believed to have targeted NATO, Ukraine, Poland and European industries in 2014 (Russian Hackers 2016).
- A city within the Australian state of Queensland found that a computer rejected for a job with local government decided to seek revenge by hacking into the city's wastewater management system. During a 2-month period, he directed computers to spill hundreds of thousands of gallons of raw sewage into local rivers, parks, and public areas before authorities were able to identify him as the perpetrator (Janke *et al*. 2014).
- A major cyber-security problem occurred in the City of Bacon Raton, Florida, a medium sized water and wastewater facility. The utility experienced a series of cyber-security

COLOR ONLINE AND BW IN PRINT

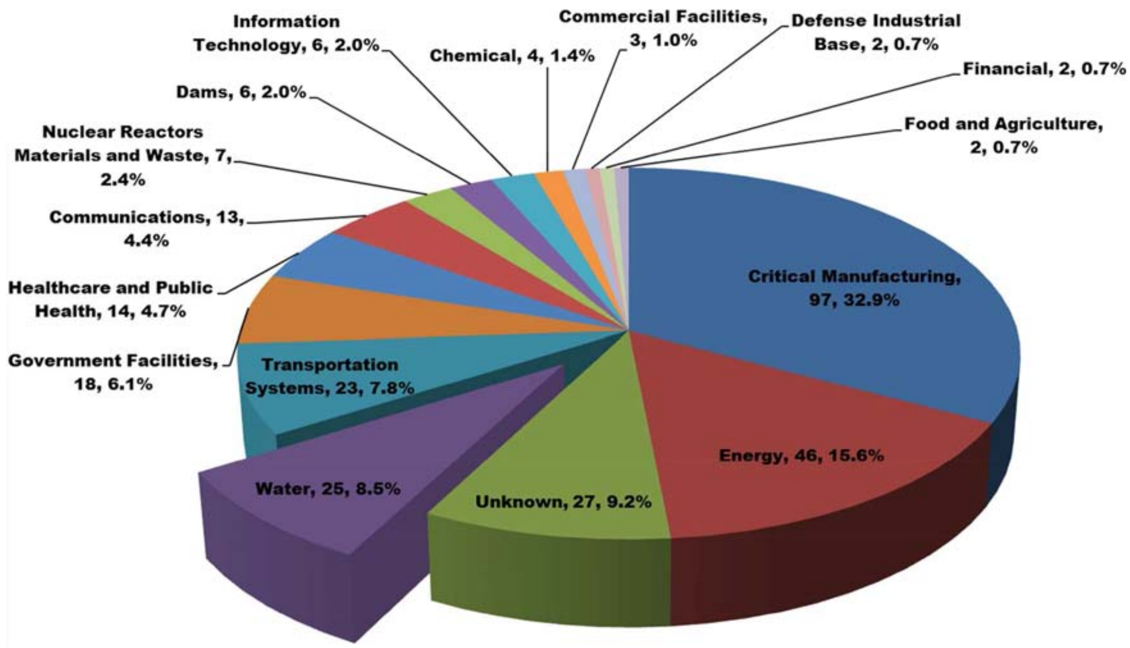



**Fig. 1.** 2015 Cybersecurity incidents reported by sector (DHS 2016). [Colour figure can be viewed at wileyonlinelibrary.com]



incidents resulting in plant shutdowns. Eventually the SCADA system locked-up and caused the water plant to shut down and it took 8 h to re-establish control of the system. There was no monitoring system for the network traffic so it was difficult to diagnose the source of the problem. Ultimately it was concluded that the network had experienced a data storm. Eventually the utility was able to update the SCADA system without losing any of the systems functionality (Horta 2007).

## Protecting water and wastewater systems in the United States

SCADA/ICS systems are an essential component for the effective operation of most water and wastewater utilities in the US Homeland Security Presidential Directive 7 (HSPD–7 2002) and its successor, the Presidential Policy Directive issued in 2013 (PPD-21 2013). The Water Sector has been identified as one of the 16 CI sectors that must be protected.

F1 Figure 1 shows that, in 2015, the DHS responded to 245 incidents. The Water sector reported the fourth largest number of incidents resulting in DHS incident response support (DHS 2016). The Energy sector reported the second largest number of reported incidents. Clearly these incidents could have a direct impact on water supply systems.

The US Environmental Protection Agency (EPA), is the sector-specific agency lead for protecting the CI in the Water Sector. EPA works collaboratively with the DHS, utility owners and operators and representatives from industry associations to ensure that cyber-protection and resilience strategies are effective and practical (EO 13636 2016). EPA has determined that current cybersecurity regulatory requirements in the Water Sector are sufficient and contemplates no regulatory action.

Sector-specific partners include: the EPA, DHS, the National Institute for Science and Technology (NIST), the American Water Works Association (AWWA), the Water Research Foundation, the Water Environment Research Foundation and other water associations, educational institutions, national research laboratories, public and private research foundations, states/local agencies, PWSs and related organizations.

The water utility industry has been active in a number of ways to improve cyber-security in the industry. For example, the Virginia Department of Health in collaboration with USEPA Region 3 has undertaken an evaluation of cybersecurity practices in 24 utilities of varying size and characteristics (Manalo *et al*. 2015). In California various water districts have formed a committee to take the lead in promoting awareness of cyber-security throughout the State's public water utilities (Johnson & Edwards 2007).

For example, in an effort to provide PWSs with more actionable information on cybersecurity, AWWA has released the Process Control System Security Guidance for the Water Sector (AWWA 2014) and a supporting Use-Case Tool (Roberson & Morley 2014). The goal of AWWA's guidance is to provide water sector utility owners/operators with a consistent and repeatable course of action to reduce vulnerabilities to cyber-attacks as recommended by the American National Standards Institute (ANSI)/AWWA G430 and the Executive Order 13636 (EO 13636 2016).

The ANSI/AWWA G430 (AWWA 2015) standard defines the minimum requirements for a protective security program for the Water Sector. The standard promotes the protection of employee safety, public health, public safety and public confidence. This standard is one of several in the AWWA Utility Management series designed to cover the principal activities of a typical public water system. This AWWA standard has received the SAFETY Act designation from the DHS in February 2012.

The G430 standard applies to all water and wastewater systems regardless of size, location, ownership or regulatory status. This standard build on the long-standing drinking water sector practice of using a 'multiple barrier approach' to protect public health and safety. The requirements of this standard support a utility-specific security program and are expected to result in consistent and measurable outcomes. They address the full spectrum of risk management including organisational commitment, physical and cyber-security and emergency preparedness.

### Common vulnerabilities in the water supply industry

Historically, business and SCADA networks were separate. Even if a utility owner recognised the value of integrating SCADA data into their strategic decision-making support systems, limitations in network topologies made integration difficult. Older SCADA systems relied heavily on serial connectivity and very low frequency radio communications that could provide enhanced range and partial line-of-sight connectivity, none of which supported standard internet protocol (IP) connectivity desired by business networks (Panguluri *et al*. 2011). This virtual isolation has led to a false sense of security by many SCADA system administrators. Increasingly, however, SCADA and business networks of most medium-to large-scale PWSs are inter-connected to provide integrated operation. If such integration is not secured, it will generally lead to greater vulnerability; this is very important to the water sector because it is thought to lag behind most other CIs in securing its control systems (Baker *et al*. 2010; Weiss 2014). The top five areas of common security gaps in water supply are: (1) network configurations, (2) media protection, (3) remote access, (4) documented policies and procedures, and (5) trained staff.

A hacker, depending on motive and objectives, may try to extract information (data) to further develop attacks or sell the information for gain. In terms of water systems, an objective may be to cause public distrust or fear, the hacker may attempt to deny access to the system and/or destroy equipment. Hackers will often change files to cover their tracks to be undetectable. Cyber-impacts may also have process impacts depending on the process and system design. For instance, if attackers change database parameters in the real-time database (impacts system integrity), they could turn on pumps potentially causing a tank to overflow as illustrated by the successful attack against the wastewater treatment plant in the Maroochy Shire in Queensland, Australia (Panguluri *et al*. 2004; Janke *et al*. 2014; Weiss 2014).

## Protecting drinking water systems

### Creating a cybersecurity culture

Many water managers are unfamiliar with information technology (IT) and SCADA/ICS technology, much less cybersecurity defences. Therefore, they must depend on their technical staff. However, there are steps that utility managers can take to secure their systems against cyber-attacks (Clark & Hakim 2016; Panguluri *et al*. 2016). Fisher (2014) lists an eight-stage process for creating major change:

- Establishing a sense of urgency by identifying the potential crises.
- Creating the guiding coalition by putting together a group with the power to lead change.
- Developing a vision and strategy including policies and procedures to define and enforce security.
- Communicating the change vision.
- Empowering broad-based action.
- Generating short-term wins.
- Consolidating gains and producing more change.
- Anchoring new approaches in the emergent culture.

Establishing a cyber-security culture is the framework for implementing a strong defensive program. It puts the three legs of cyber-security on a firm foundation, namely, technology, people and physical protection. The last of these items implies locating IT equipment in a safe location.

### Secured network design

It has been traditional for industrial control systems to apply standard IT security systems to control networks, including physical security, personnel security and ICS network perimeter protections including firewalls and network intrusion detection systems (NIDS). However, a Ponemon Institute study (Ponemon Institute LLC 2013) found that malicious cyber breaches took an average of 80 days to detect, and 123 days to resolve. An example of a technological approach that may protect an ICS is a unidirectional gateway. Therefore, many experts recommend that technological innovations such as unidirectional gateways be used as the modern alternative to firewall perimeter protections for ICSs (Waterfall 2016). Figure 2 illustrates a unidirectional gateway deployment. All unidirectional gateways are combinations of F2

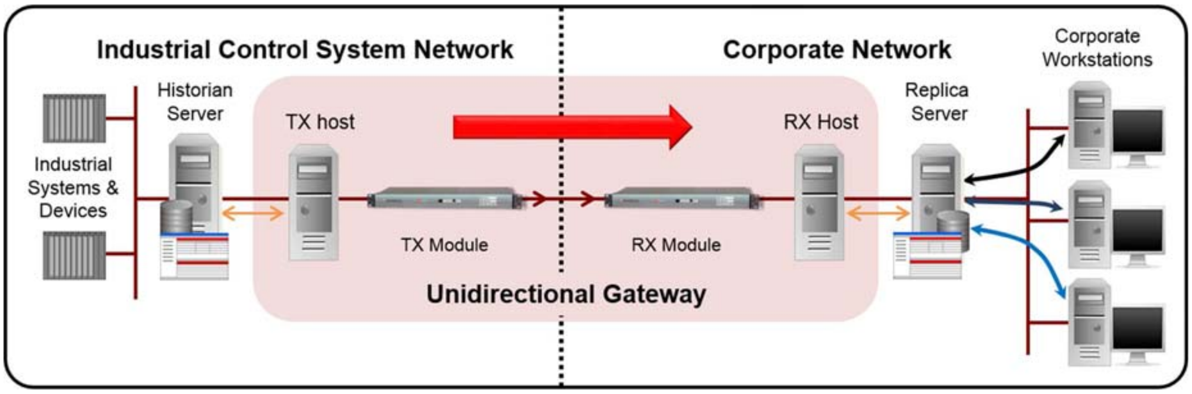



**Fig. 2.** Example of a unidirectional network (Ginter 2016). [Colour figure can be viewed at wileyonlinelibrary.com]

hardware and software as shown below. A possible approach is a unidirectional gateway which results in a system able to transmit information from a protected individual network, but physically unable to transmit any information back to that protected network from outside the system.

In cases where a unidirectional gateway is unaffordable (e.g., in smaller-sized utilities) or is technically challenging to implement, utilities should investigate other alternatives such as implementing virtual routing and forwarding (VRF) (Stack 2015). VRF technology is included with some off-the-shelf routers that allow different routing tables to work simultaneously within a given router. Devices using the different routing tables are virtually isolated, unable to communicate with each other even though they are connected to the same hardware. This allows network paths to be virtually segmented without using multiple devices. Internet service providers often take advantage of VRF functionality to create separate virtual private networks (VPNs) for customers. This technology is also referred to as VPN routing and forwarding.

Cybersecurity designs should strive to limit access or incorporate isolation capabilities of ICS/SCADA systems. The isolation of an ICS system can be achieved by establishing security enclaves (or zones) with virtual local area networks (VLANs) or subnets that are segregated from lower security zones like corporate networks or any Internet accessible zones. Information passing from one security zone to another should be monitored. Figure 3 illustrates an example of a secure PWS architecture. F3

In this example, the ICS environment has been isolated with no ingress electronic connections. The use of data





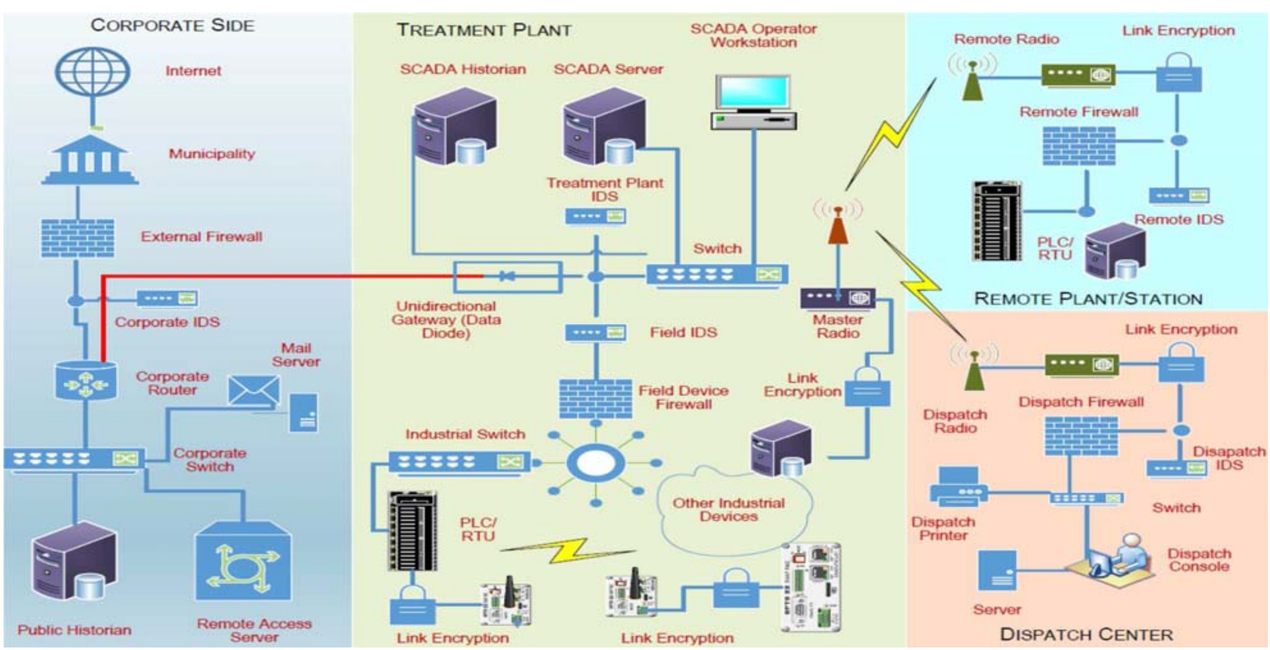



**Fig. 3.** Secure PWS architecture example (Panguluri *et al*. 2016). [Colour figure can be viewed at wileyonlinelibrary.com]

diodes between the SCADA/ICS (process control) and corporate (business analytics, payroll, accounting, email, etc.) IT environments allows for information sharing from the ICS environment through a truly one-way transfer of data from ICS historians (databases) for business needs and reporting.

The use of true isolation through data-diode technologies between the treatment plant ICS and the corporate environment (Fig. 3) is more recent. The adoption of this technology within the water sector has been observed by the authors at one utility but is gaining increasing acceptance within the water sector. Some PWSs have identified the use of this technology in their advance security posture planning documents. However, the implementation of this technology requires an investment in both capital and labour. At least two full-time-equivalent (FTE) technology staff are typically required for several months during the development, testing, verification and deployment phases. Additionally, depending upon the complexity of the architecture, a successful deployment may require three or more FTEs. After the full implementation and optimisation of the secure PWS architecture, at least $^1/_4$ to $^1/_2$ FTE will be necessary to manage and support this type of security posture. Based on current water sector cybersecurity implementation and execution costs, it is estimated that this technology implementation (depending on the features) would average around $300 000 for initial implementation and optimisation.

The application of secure architecture and isolation of the ICS environment prevents both remote access connection and unauthorised computers or network devices including third party vendors from entering into the ICS environment. Furthermore, the utility will also need to address the issue of securely installing patches, anti-virus signature files and application updates. These approaches typically involve the use of portable media (USB memory and USB hard drives) which present security concerns. By deploying unidirectional gateways (based on data Diode technology) the cyber risk of compromise from external networks, like the internet, is significantly reduced if not eliminated. However, trusted insiders, portable media, and physical intrusions still present a potential vector into the system. Therefore, a strong media protection policy, as well as strong physical controls needs to be developed to maintain the integrity of the environment. Prior to adding a network device or computer to the ICS environment, a thorough analysis should be conducted. Once approved, the equipment should stay at a secure off-site location for future use and identified as an ICS component.

The suggested architecture along with strong policies and procedures is necessary in order to develop a security culture that raises the level of awareness of each employee. Management should provide all necessary training for the core cybersecurity staff. The next stage in security is to monitor and verify that the security controls are working as designed through monitoring and log-file analysis. Systems, applications and security components should enable logging. This capability should be centrally located through a security information and event management system to allow central management of monitoring appliances. It should include log-reviews and alerting capabilities in the event that the system starts to identify anomalies with the systems for early detection, alerting and recovery capabilities.

Finally, when excessing or decommissioning equipment, a proper equipment disposal process should be in place to ensure no proprietary information ever leaves the environment. A proper disposal process protects from malicious reverse engineering, discovery and reconnaissance activities.

## Summary and conclusions

As infrastructure becomes increasingly connected, cyber-physical security in CI such as water supply will become an even greater concern. In the United States, cyber-security issues are extremely important from a national security perspective (US GAO 2013); however, there is a strong desire for the separation of powers between the Federal government and the individual States that has made developing a unified cyber-security strategy difficult.

It is clear that cyber threats to the water sector are real. The insider attack on the Maroochy Shire wastewater treatment plant provides an insight into the real consequences of a specific attack and there have been confirmed cases of cyber-attacks against domestic water utilities. Such attacks could affect public health and increase distrust of government, by delivering contaminated water that could potentially cause sickness without detection.

In the United States virtually all drinking water utilities, even subdivision-sized systems, have become dependent on SCADA systems. It is therefore imperative that PWSs adopt suitable countermeasures to prevent or minimise the consequences of cyber-attacks. Establishing a strong cyber-security environment is the basis for implementing a strong cyber-defence. Such a program should consist of technology, people and physical protection, where the last refers to physical protection of cyber-devices from physical tampering. It is also critical that utility management create and support a cyber-security culture. The lack of policies and procedures may pose a significant barrier to developing adequate cyber-security; if management support is lacking, there will never be an effective cyber-security culture.

Utilities in the United States should avail themselves of the free opportunities available through the US DHS to train their staff and allocate necessary funding to achieve improvements in cybersecurity. The greatest challenge for the water industry is the large variance in system size, staffing, and resources available to the individual utilities.

Utilities should adopt countermeasures that best meet their security and organisational requirements. AQ6

## Acknowledgement

The authors would like to acknowledge the assistance of Trent D. Nelson, and Richard P. Wyman of the Idaho National Laboratory, Idaho Falls, ID in preparing this manuscript.

To submit a comment on this article please go to http://mc.manuscriptcentral.com/wej. For further information please see the Author Guidelines at wileyonlinelibrary.com

## References

American Water Works Association (AWWA). (2014) *Process Control System Security Guidance for the Water Sector*. ~~Author~~, Washington, DC. AQ7

American Water Works Association (AWWA). (2015) *Security Practices for Operation and Management*. ~~Author,~~ Denver, CO.

Baker, S., Waterman, S. and Ivanov, G. (2010) *In the Crossfire – Critical Infrastructure in the Age of Cyber War*. A global report on the threats facing key industries. McAfee International Ltd, London, UK.

Bush, G.W. (2003) *National Strategy to Secure Cyberspace*. The White House, Washington, DC.

Clapper, J.R. (2012) *Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*. Office of the Director of National Intelligence, Washington, DC.

Clark, R.M. and Hakim, S. (2016) Protecting Critical Infrastructure at the State Provincial and Local Level: Issues in Cyber-Physical Security. *In* Clark, R.M. and Hakim, S. (eds). *Cyber-Physical Security at the State, Provincial, and Local Level: Protecting Critical Infrastructure*, pp. 1–17. Springer International Publishers, Switzerland.

Dakin, R., Newman, R. and Groves, D. (2009) The Case for Cyber Security in the Water Sector. *J. Am. Water Works Assoc.*, **101**, 30–32.

Department of Homeland Security (DHS). (2016) NCCIC/ICS-CERT Year in Review. National Cybersecurity and Communications Integration Center/Industrial Control Systems Cyber Emergency Response Team FY 2015. Issued by DHS's National Cybersecurity and Communications Integration Center. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf [accessed on 25 January 2018].

Edwards, D. (2010) Robust ICSs Critical for Guarding against Cyber Threats. *J. Am. Water Works Assoc.*, **102**, 30–33.

EO 13636. (2016) Executive Order 13636: Improving Critical Infrastructure.https://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical [accessed on 25 January 2018].

Fischer, E.A., Liu, E.C., Rollins, J. and Theohary, C.A. (2013) The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress. Congressional Research Service. https://www.crs.gov [accessed on 25 January 2018].

Fisher, R. (2014) Applying Culture Change in Cyber Security to Enhance Homeland Security. *Colorado Technical University Doctoral Symposium*, October 16. Colorado Technical University, Colorado Springs, CO.

Ginter, A.P. (2016) Cyber Perimeters for Critical Infrastructures. *In* Clark, R.M. and Hakim, S. (eds). *Cyber-Physical Security at the State, Provincial, and Local Level: Protecting Critical Infrastructure*, pp. 67–100. Springer International Publishers, Switzerland.

Homeland Security Presidential Directive 7 (HSPD–7). (2002) *Directive on Critical Infrastructure Identification, Prioritization, and Protection*. Issued by the White House, December 17, 2003.

Horta, R. (2007) Final Report-The City of Boca Raton: A Case Study in water Utility Cybersecurity. *J. Am. Water Works Assoc.*, **99**, 48–50.

Janke, R., Tryby, M.E. and Clark, R.M. (2014) Protecting Water Supply Critical Infrastructure: An Overview. *In* Clark, R.M. and Hakim, S. (eds). *Securing Water and Wastewater Systems: Global Experiences*, pp. 29–85. Springer International Publishers, Switzerland.

Johnson, S. and Edwards, D. (2007) Why Water and Wastewater Utilities Should Be Concerned About Cyber Security. *J. Am. Water Works Assoc.*, **99**, 89–94.

Lipton, E., Sanger, D.E. and Scott, S. (2016) The Perfect Weapon: How Russian Cyber Power Invaded the US. http://www.nytimes.com/2018/12/13/us politics/russia-hack-election-dnc.html?_r=0 [accessed on 25 January 2018].

Manalo, C., Noble, T., Miller, K. and Ferro, C. (2015) Control Systems Cybersecurity: Lessons Learned From Virginia Assessment. *J. Am. Water Works Assoc.*, **107**, 60–67.

National Governors Association(NGA). (2015) About What is the National Governors Association? http://www.nga.org/cms/about [accessed on 25 January 2018].

National Institute of Standards and Technology (NIST). (2014) Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0, National Institute of Standards and Technology http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed on 25 January 2018) AQ8

Obama, B. (2009) *Remarks by the President on Securing Our Nation's Cyber Infrastructure*. Office of the Press Secretary, Washington, DC.

Panetta, L.E. (2012) *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security*. Secretary of Defense, New York, NY.

Panguluri, S., Nelson, T.D. and Wyman, R.P. (2016) Creating a Cybersecurity Culture for your Water/Waste Water Utility. *In* Clark, R.M. and Hakim, S. (eds). *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, pp. 133–159. Springer International Publishers, Switzerland.

Panguluri, S., Phillips, Jr. W.R. and Clark, R.M. (2004) Cyber Threats and IT/SCADA System Vulnerability. *In* Mays, L.W. (ed). *Water Supply Systems Security*, pp. 5.1–5.18. McGraw-Hill, New York, NY.

Panguluri, S., Phillips, Jr. W.R. and Ellis, P. (2011) Cyber security: Protecting Water and Wastewater Infrastructure. *In* Clark, R.M., Hakim, S. and Ostfeld, A. (eds). *Handbook of Water and Wastewater Systems Protection*, pp. 285–318. Springer International Publishers, Switzerland.

Ponemon Institute LLC. (2013) *The Post Breach Boom, Waterfall Security Solutions. Introduction to Waterfall Unidirectional Security Gateways: True Unidirectional, True Security*. AQ9

Presidential Policy Directive-21 (PPD-21). (2013) Critical Infrastructure Security and Resilience. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [accessed on 25 January 2018].

Roberson, J.A. and Morley, K.M. (2014) A Simple Action Plan for Utilities to Secure Their Process Control Systems. *J. Am. Water Works Assoc.*, **106**, 23–25.

Russian Hackers. (2016) Russian Hackers are Suspected in a Cyber Attack that Caused a Huge Blackout in Ukraine.http://qz.com/587520/russian-hackers-are-suspected-in-a-cyber-attack-that-caused-a-huge-blackout-in-ukraine [accessed on 25 January 2018].

Stack 8. (2015) Networking Segmentation for Security using VRF.http://info.stack8.com/blog/enterprise-networking-segmentation-for-security-using-vrf [accessed on 25 January 2018].

Tabansky, L. (2016). Cyber Security Challenges: The Israeli Water Sector Example. *In* Clark, R.M. and Hakim, S. (eds). *Cyber Physical Security: Protecting Critical Infrastructure at the State and Local Level*, pp. 205–219. Springer International Publishers, Switzerland.

United States Government Accountability Office (US GAO). (2011) *High Risk Series: An Update*. GAO-11–278. Author, Washington, DC.

United States Government Accountability Office (US GAO). (2013). *Cybersecurity National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*. GAO-13–187. Author, Washington, DC.

Waterfall. (2016) Unidirectional Security Gateways. http://waterfall-security.com/products/unidirectional-security-gateways. [accessed on 25 January 2018].

Weiss, J. (2014) Industrial Control System (ICS) Cyber Security for Water and Wastewater Systems. *In* Clark, R.M. and Hakim, S. (eds). *Securing Water and Wastewater Systems, Protecting Critical Infrastructure*, pp. 87–105. Springer International Publishing, Switzerland.