A Review of Cybersecurity Incidents in the Water Sector

Amin Hassanzadeh, Ph.D.[1]; Amin Rasekh, Ph.D.[2]; Stefano Galelli, Ph.D., M.ASCE[3];
Mohsen Aghashahi, S.M.ASCE[4]; Riccardo Taormina, Ph.D.[5];
Avi Ostfeld, Ph.D., F.ASCE[6]; and M. Katherine Banks, Ph.D., F.ASCE[7]

Abstract: This study presents a critical review of disclosed, documented, and malicious cybersecurity incidents in the water sector to inform safeguarding efforts against cybersecurity threats. The review is presented within a technical context of industrial control system architectures, attack-defense models, and security solutions. Fifteen incidents were selected and analyzed through a search strategy that included a variety of public information sources ranging from federal investigation reports to scientific papers. For each individual incident, the situation, response, remediation, and lessons learned were compiled and described. The findings of this review indicate an increase in the frequency, diversity, and complexity of cyberthreats to the water sector. Although the emergence of new threats, such as ransomware or cryptojacking, was found, a recurrence of similar vulnerabilities and threats, such as insider threats, was also evident, emphasizing the need for an adaptive, cooperative, and comprehensive approach to water cyberdefense. **DOI: 10.1061/(ASCE)EE.1943-7870.0001686.** *© 2020 American Society of Civil Engineers.*

Introduction

The water and wastewater sector (WWS) is considered by the US Department of Homeland Security (DHS) to be one of the main targets for cyberattacks among the 16 lifeline infrastructure sectors (White House 2013). Safeguarding it against cybersecurity threats is considered a matter of national priority (White House 2017). From 2012 to 2015, WWS received the highest number of assessments from the Cybersecurity and Infrastructure Security Agency Industrial Control Systems Cyber Emergency Response Team (ICS-CERT 2016b), which routinely conducts on-site cybersecurity assessments for several critical infrastructure sectors (ICS-CERT 2016b). The only exception was 2014, when the number of assessments in the energy sector was slightly higher (ICS-CERT 2016b).

According to ICS-CERT (2016b), 25 water utilities reported cybersecurity incidents in 2015, making WWS the third most targeted sector. Because there are over 151,000 public water systems in the United States (USEPA 2019a), one may conclude that cybersecurity risk in WWS is low, and most systems are secure. However, the reality is that many cybersecurity incidents either go undetected, and consequently unreported (Walton 2016), or are not disclosed—because doing so may jeopardize the victim's reputation, customers' trust, and, consequently, revenues (Cava 2018; Rubin 2019). Moreover, the complexity and impact of cyber-originated incidents can be as serious as the incidents initiated from the operational technology (OT) area. Most industrial sectors, and WWS in particular, now are embracing the digital age, but still lack dedicated cybersecurity specialists to provide customized security guidelines, secure systems, and train employees.

Recently, cybersecurity has piqued the interest and attention of the WWS industry and policy-making entities. Several educational programs have been offered by the USEPA, DHS, the American Water Works Association, and the Water Information Sharing and Analysis Center over the last few years to raise awareness, train staff, and provide resources and tools to assist with cybersecurity practices (WaterISAC 2015; ICS-CERT 2019; USEPA 2019b). This has been accompanied by a rising interest in the research community (Amin et al. 2013; Rasekh et al. 2016; Ahmed et al. 2017; Formby et al. 2017; Taormina et al. 2017, 2018; Laszka et al. 2017; Chandy et al. 2018; Taormina and Galelli 2018; Housh and Ohar 2018; Ramotsoela et al. 2019). In this respect, valuable lessons and insights may exist in past cybersecurity incidents that should be discovered and disseminated to inform the ongoing cyberdefense investments and efforts, thereby enhancing their relevance and effectiveness. This requires a comprehensive compilation and review of the these incidents, a public resource that is not currently available.

This study, conducted by the Environmental and Water Resources Institute (EWRI) Task Committee on Cyberphysical Security of Water Distribution Systems, presents a review of disclosed, documented, and malicious cybersecurity incidents in WWS to inform safeguarding efforts against cybersecurity threats. First, a review of a typical industrial control system (ICS) architecture, standard models, and common practices, alongside security controls and solutions offered for these environments, is provided. This is followed by a description of attack-defense models, which are an important concept in the design of cybersecurity systems. Next, a selection of cyber incidents in WWS is presented. The main details regarding the situation, response, remediation, and lessons learned are reported for each incident. This review concludes with recommendations for industry, policy makers, and research community.

[1] R&D Principal, Accenture Labs, Cyber Fusion Center, 800 North Glebe Rd., Arlington, VA. Email: amin.hassanzadeh@accenture.com

[2] Industry Advisor, Zachry Dept. of Civil Engineering, Texas A&M Univ., 400 Bizzell St., College Station, TX 77843 (corresponding author). ORCID: https://orcid.org/0000-0003-3102-0525. Email: aminrasekh@outlook.com

[3] Assistant Professor, Pillar of Engineering Systems and Design, Singapore Univ. of Technology and Design, 8 Somapah Rd., Singapore 487372. ORCID: https://orcid.org/0000-0003-2316-3243

[4] Doctoral Student, Zachry Dept. of Civil Engineering, Texas A&M Univ., 400 Bizzell St., College Station, TX 77843.

[5] Assistant Professor, Faculty of Civil Engineering and Geosciences, Dept. of Water Management, Delft Univ. of Technology, Stevinweg 1, 2628 CN Delft, Netherlands.

[6] Professor, Faculty of Civil and Environmental Engineering, Technion–Israel Institute of Technology, Haifa 32000, Israel.

[7] Professor, College of Engineering, Texas A&M Univ., 400 Bizzell St., College Station, TX 77843.

Note. This manuscript was published online on February 28, 2020. Discussion period open until July 28, 2020; separate discussions must be submitted for individual papers. This paper is part of the ***Journal of Environmental Engineering***, © ASCE, ISSN 0733-9372.

Industrial Control Networks

To provide context for the analysis of the incidents, this section reviews traditional OT networks, their integration with information technology (IT) networks, and standard architecture designs proposed for ICS networks. We refered to these architectures when reviewing some of the incidents and mapped the attacker's activities to the architectural layers and targeted hardware/software.

ICS networks traditionally use a system of hardware and software components—called Supervisory Control and Data Acquisition (SCADA)—for process control, data collection, system monitoring, communication with industrial devices, and log data storing. A traditional ICS architecture is depicted in Fig. 1(a). The lowest level generally consists of field elements (also called end or dumb devices), such as sensors, pumps, and actuators. These elements are operated by control devices, such as programmable logic controllers (PLC) and remote terminal units (RTU). PLCs and RTUs are microcomputers that send control signals to the field elements, acquire data, and transmit them to the central control station, such as a master terminal unit (MTU). MTU and RTUs/PLCs communicate and function in a master/subordinate model (through wired or wireless networks, public telephone networks, or even through the internet) to send commands, upload new configurations, and monitor the field elements. Operators manage all these operations through a human–machine interface (HMI) connected to the MTU that allows them to gather data, send commands to remote sites, and change settings and configurations (Krutz 2005).

Fig. 1(b) shows a typical water system architecture with RTUs and PLCs geographically dispersed at different sites. We mapped different layers of a SCADA architecture to this sample network, in which field elements are monitored by RTUs with wireless antennas. The SCADA servers are located in a central control station (e.g., the headquarters of a water utility) and remotely communicate with the RTUs and PLCs scattered throughout the entire service area (SWAN Forum Interoperability Workgroup 2016).

For many years, SCADA systems, and, in general, OT networks in industrial environments, were air-gapped—that is, not connected to corporate IT networks or the internet. However, as technology advanced, many organizations consolidated overlapping IT and OT networks. This approach aims at saving maintenance costs and integrating data collection and analysis (Krutz 2005). However, such integration comes at high security risks for the following reasons: (1) OT networks have different operational priorities than IT networks—e.g., availability versus confidentiality—and one model may not fit both purposes; (2) most ICS devices and protocols are not designed to support security features such as data encryption or access control, and often support remote access through radio modems; (3) expensive legacy devices in ICS environments provide limited visualization options to implement and evaluate security modifications; and (4) critical and real-time business operations in OT, along with safety regulations, prevent immediate implementation of remediation options that may require system interruptions. For these reasons, security experts have proposed some work-around options to limit the access of users to the OT network. Other efforts in the ICS security field include constantly-improving standards, protocols, and devices to support security features.

The new generation of converged IT-OT networks in industrial control systems, also referred to as the industrial internet of things (IIoT), is no longer air-gapped. Fig. 1(c) depicts a typical integrated ICS network consisting of multiple levels and zones, also known as the Industrial Automation and Control Systems (IACS) security standard [ISA-62443 (International Society of Automation 2009); Krutz 2005]. A zone is in fact a set of assets (IT or OT devices) grouped together to provide a subclass of services and applications for the entire ICS network. The main zones can be described as follows:

- The enterprise zone includes assets for business logistics and enterprise systems, representing Levels 4 and 5, respectively. This zone is also known as IT network.
- The demilitarized zone (DMZ) separates IT and OT networks, thus preventing direct access to OT devices from the IT network.

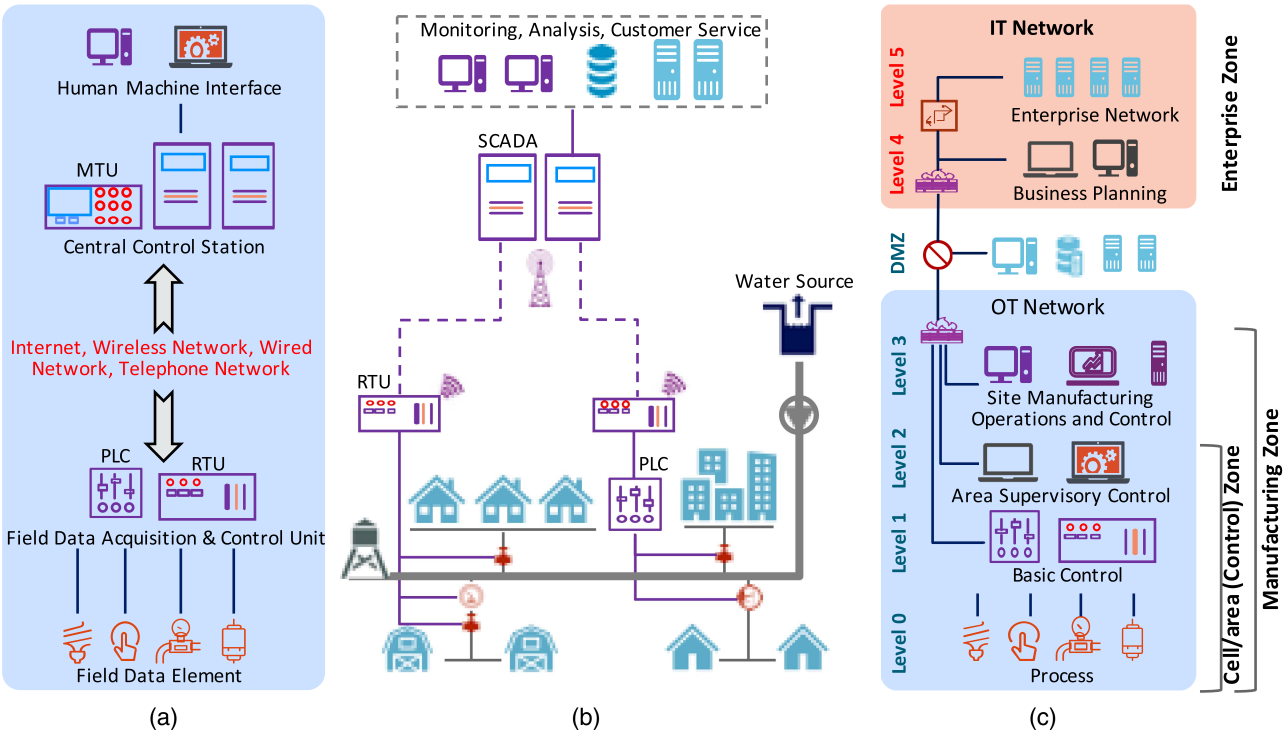


Fig. 1. (a) Traditional ICS architecture; (b) typical architecture in water systems; and (c) ISA-62443 zoned architecture.

All corporate-accessible services (e.g., web and email) reside in this zone.

- The manufacturing zone and control zone, in which the former refers to the entire OT domain, including Levels 0, 1, 2, and 3, and the latter refers to Levels 0, 1, and 2. Control zone is thus equivalent to the traditional ICS architecture in Fig. 1(a). Level 3 provides site-level operation and asset management. Plant historian, production scheduling and reporting, and patch and file services reside at Level 3 (Hassanzadeh et al. 2015).

Attack and Defense Models

The incidents reviewed in this paper can be comprehended more effectively with some knowledge of attack and defense models, which are introduced next.

Attack Models

From the attacker's perspective, a systematic process consisting of several steps or individual malicious activities is required to obtain the desired effect on the victim's network. Lockheed Martin researchers have expanded the kill chain concept used in military applications to define the cyber kill chain (CKC) (Hutchins et al. 2011), which models the life cycle of an attack based on the fact that the adversary uses a series of malicious activities (also called intrusions or single-step attacks) and adjusts each step based on the success or failure of the previous step. CKC steps are defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives. Inspired by the CKC model, researchers have proposed several attack life-cycle models, which were reviewed and discussed by Hassanzadeh and Burkett (2018).

In industrial environments, the attack life cycle is slightly different because of the different architecture design [Fig. 1(c)]. The target in such networks can be an asset in one of the three domains, namely, IT, DMZ, or OT. However, in most reported ICS incidents, the target is an OT asset (Hassanzadeh et al. 2015), because the attacker gains access to the victim's environment through the IT domain and then traverse to the OT infrastructure by launching multiple attacks. This model is defined as the ICS kill chain, a multidomain, multistep approach that considers ISA-62443 architectural levels and CKC steps together. Because the attacker may need to repeat several CKC steps at each IT/OT level to laterally move within the network from one asset to another (until he/she reaches the target), Hassanzadeh and Burkett (2018) proposed a spiral attack model to accurately describe the attacker's activities within converged IT/OT systems. Fig. 2(a) shows a simplified version of this model, which is color-coded to map it to the IT/DMZ/OT domains of Fig. 1(c). An attacker may start with some reconnaissance activities in outer layers of an organization that are more exposed to the public (e.g., web server or mail server), and then find a vulnerable host that can be exploited. Once the first attack is delivered and executed, the attacker is already inside the victim's network, and then escalates his/her privileges and moves laterally within the network toward the final target, which is placed in the lower levels. This is a generic model, so there might be attacks that do not necessarily start from Level 5—such as an insider who uses OT workstations or a vulnerable server in the DMZ to launch an attack.

Because an attacker operates in a chain of events (i.e., a set of single-step intrusions), the diamond model of intrusion analysis proposes a formal method called activity thread (Caltagirone et al. 2013). The method shows not only the attacker's steps and the causal relation between them, but also a complete list of features for each of these steps. Fig. 2(b) shows the core and metafeatures of each single-step intrusion, or event. An activity thread in an industrial environment is a directed graph [such as the spiral set of arches in Fig. 2(a)], in which each vertex is an event/intrusion [Fig. 2(b)] and links represent the relation between those intrusions from the first step of the attack to the final target. The four core features describe how an adversary deploys a capability over some infrastructure against a victim [Fig. 2(b)]

- An adversary is the actor or organization responsible for the attack. The adversary can be categorized as an insider or outsider and as an individual, group, or organization. This usually is an unknown feature in most cyberattacks. It is important to understand the distinction between adversary operator (i.e., the actual hacker) and adversary customer (i.e., the entity that benefits from the attack).

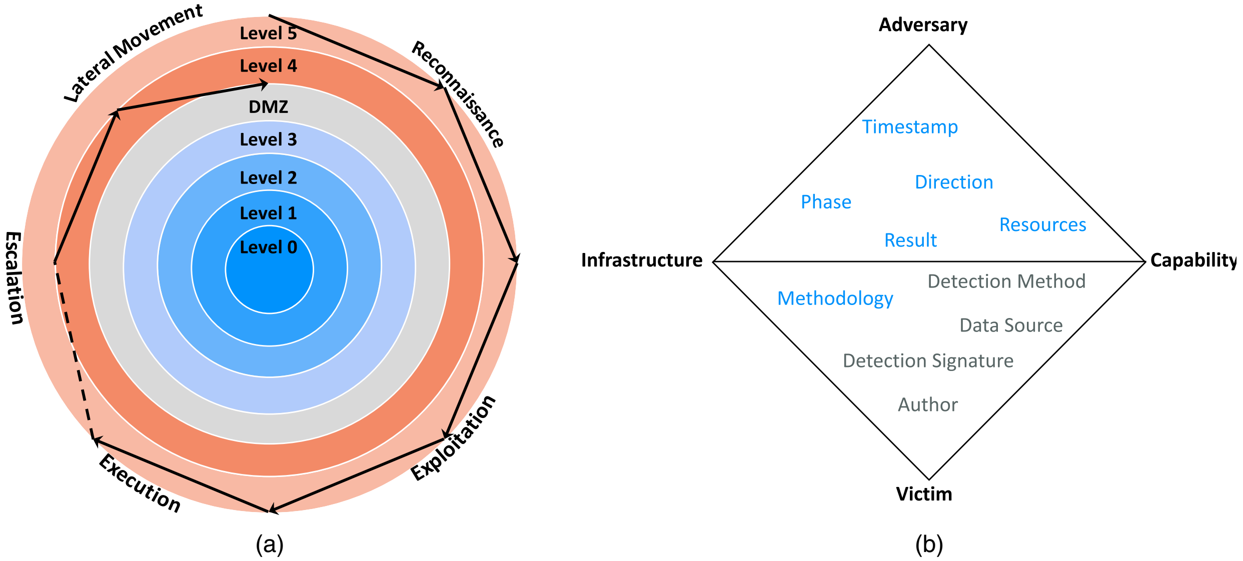


Fig. 2. (a) Spiral attack model in converged IT/OT networks; and (b) diamond model of intrusion analysis, with the core features at the corners, and metafeatures and expanded metafeatures inside the diamond.

- Capability is the set of tools and techniques that are used by the attacker. The vulnerabilities and configuration issues in the target environment define the capability of an attacker.
- Infrastructure is the physical and/or logical communication structure, such as email addresses or USB devices, used by the attacker to deliver the attack capabilities, maintain control over them, and finally obtain results. The infrastructure can be owned or controlled by the attacker or an intermediary (e.g., zombies hosts, botnets, or compromised email accounts).
- A victim is the target that has vulnerabilities and configuration issues to provide attack capabilities for the adversary. Victims are either persona (e.g., people or organizations) or assets (e.g., networks, systems, accounts, or information).

In addition to the core features, there are six meta-features for every security event: (1) a timestamp, that is, the start and stop time of the intrusion; (2) a phase, or step, describing the position of the intrusion in the entire attack kill chain; (3) a direction, which denotes the course of an attack (for example, data exfiltration has a victim-to-infrastructure direction, whereas probing goes from the adversary to the infrastructure); (4) a result, which indicates the status of an attack, such as success, failure, or unknown; (5) resources, such as software, hardware, information, knowledge, funds, and so forth; and (6) methodology, that is, the class of the malicious activity, such as spear-phishing or denial-of-service. Moreover, four expanded meta-features have also been used to describe a single-step intrusion: a detection method, showing what tools or techniques were used in detecting the malicious activity; a data source to detect it; a detection signature, or rule, that was used for the detection; and, an author, namely the analyst-author of the intrusion. Several multi-step attack examples and their activity threads are presented in Caltagirone et al. (2013).

Defense Models

To secure target organizations, defenders can employ several security tools and technologies. Moreover, they may have access to standards, threat intelligence databases, security controls, and benchmarks. Nonetheless, developing and implementing a thorough security strategy is a very challenging task that requires prioritization and rigor. The Center for Internet Security (CIS) proposed a list of the most fundamental and valuable security actions, called CIS controls, that every organization should consider (CIS 2019). These controls are categorized as

- basic controls, such as inventory and control of hardware/software assets, continuous vulnerability management, or controlled use of administrative privileges;
- foundational controls, such as email and web browser protections, malware defenses, or secure configuration for network devices, such as firewalls, routers, and switches; and
- organizational controls, such as the implementation of a security awareness and training program, incident response and management, penetration tests, and red team exercises.

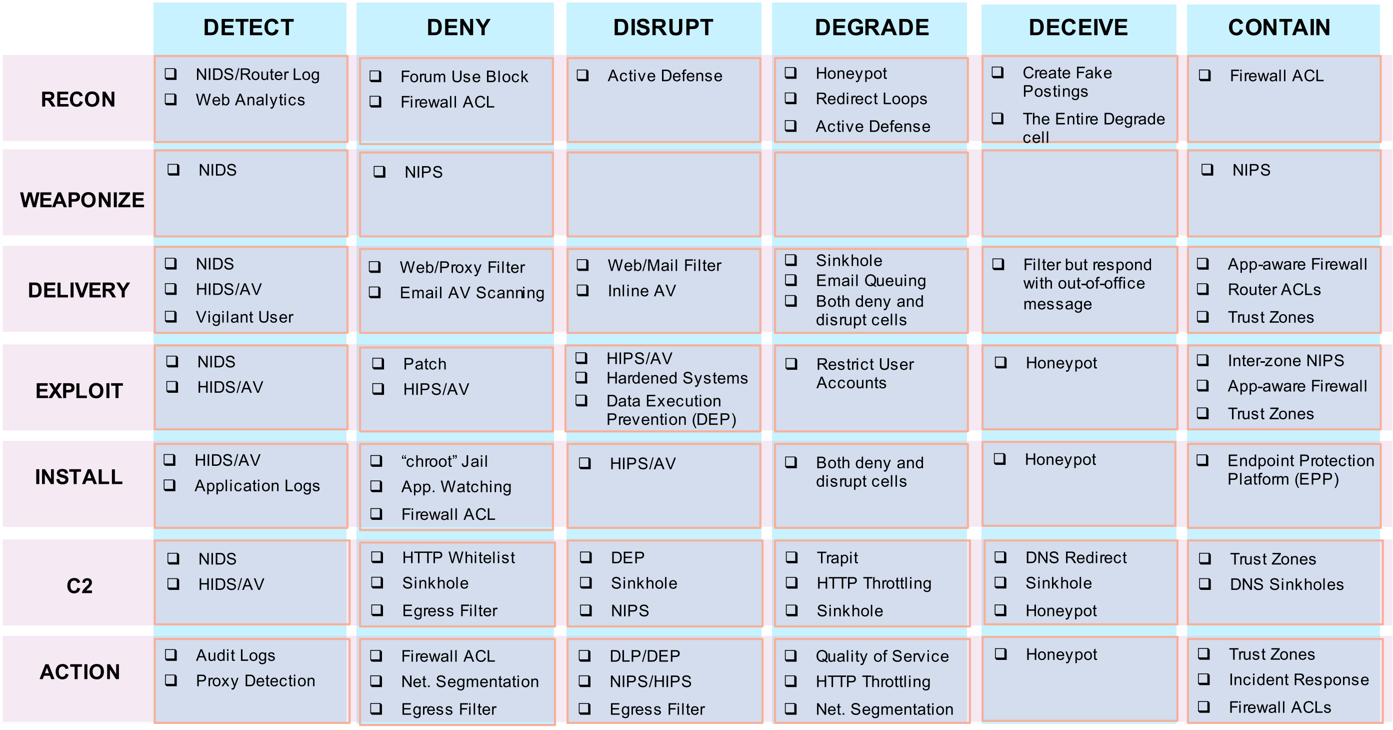
Table 1 provides the complete list of CIS controls along with their corresponding category. These controls are available and offered in different security tools and solutions. They can have various impacts depending on their goal and implementation: (1) detect the attack; (2) deny or prevent the attacker from accessing assets or information; (3) disrupt active malicious activities; (4) degrade the impact of an attack; (5) deceive the attacker; or (6) contain the malicious activity to a zone in which damages can be mitigated. Fig. 3 shows how different security controls (tools and solutions) can be used to protect an organization against an intrusion attempt at each CKC step (Hutchins et al. 2011; Bodeau et al. 2013; Willson 2013). As an example, network-based intrusion detection systems (NIDS), host-based intrusion detection systems (HIDS), or antivirus (AV) solutions can be used to detect exploitation activities. Similarly, trust zones can co3ntain malicious activities associated with multiple attack steps from delivery to action, and honeypots can deceive attackers during several attack phases. AV solutions are used mostly to detect or disrupt attacks during the delivery, exploitation, or installation phase, whereas data execution protection (DEP) techniques are used mostly as a disruption mechanism.

In addition to traditional IT-based security controls, there are several OT-specific security controls—such as data diodes or unidirectional gateways, in-line command white listing, passive asset discovery, passive OT intrusion detection (or anomaly detection), and patch and compliance management—that currently are used in

Table 1. List of CIS controls

Number	Security control	Category
1	Inventory of authorized and unauthorized devices	Basic
2	Inventory of authorized and unauthorized software	Basic
3	Secure configurations for hardware and software on mobile devices, laptops, workstations, and servers	Basic
4	Continuous vulnerability assessment and remediation	Basic
5	Controlled use of administrative privileges	Basic
6	Maintenance, monitoring, and analysis of audit logs	Basic
7	Email and web browser protections	Foundational
8	Malware defenses (installation, spread, and execution)	Foundational
9	Limitation and control of network ports, protocols, and services	Foundational
10	Data recovery capability (information back-up process)	Foundational
11	Secure configurations for network devices such as firewalls, routers, and switches	Foundational
12	Boundary defense (detect, prevent, and correct unauthorized information flow)	Foundational
13	Data protection (prevent exfiltration and ensure integrity and privacy)	Foundational
14	Controlled access based on the need to know	Foundational
15	Wireless access control (track, control, prevent, and correct wireless accesses)	Foundational
16	Account monitoring and control	Foundational
17	Security skills assessment and appropriate training to fill gaps	Organizational
18	Application software security	Organizational
19	Incident response and management	Organizational
20	Penetration tests and red team exercises	Organizational

Source: Data from CIS (2019).



	DETECT	DENY	DISRUPT	DEGRADE	DECEIVE	CONTAIN
RECON	❑ NIDS/Router Log ❑ Web Analytics	❑ Forum Use Block ❑ Firewall ACL	❑ Active Defense	❑ Honeypot ❑ Redirect Loops ❑ Active Defense	❑ Create Fake Postings ❑ The Entire Degrade cell	❑ Firewall ACL
WEAPONIZE	❑ NIDS	❑ NIPS				❑ NIPS
DELIVERY	❑ NIDS ❑ HIDS/AV ❑ Vigilant User	❑ Web/Proxy Filter ❑ Email AV Scanning	❑ Web/Mail Filter ❑ Inline AV	❑ Sinkhole ❑ Email Queuing ❑ Both deny and disrupt cells	❑ Filter but respond with out-of-office message	❑ App-aware Firewall ❑ Router ACLs ❑ Trust Zones
EXPLOIT	❑ NIDS ❑ HIDS/AV	❑ Patch ❑ HIPS/AV	❑ HIPS/AV ❑ Hardened Systems ❑ Data Execution Prevention (DEP)	❑ Restrict User Accounts	❑ Honeypot	❑ Inter-zone NIPS ❑ App-aware Firewall ❑ Trust Zones
INSTALL	❑ HIDS/AV ❑ Application Logs	❑ "chroot" Jail ❑ App. Watching ❑ Firewall ACL	❑ HIPS/AV	❑ Both deny and disrupt cells	❑ Honeypot	❑ Endpoint Protection Platform (EPP)
C2	❑ NIDS ❑ HIDS/AV	❑ HTTP Whitelist ❑ Sinkhole ❑ Egress Filter	❑ DEP ❑ Sinkhole ❑ NIPS	❑ Trapit ❑ HTTP Throttling ❑ Sinkhole	❑ DNS Redirect ❑ Sinkhole ❑ Honeypot	❑ Trust Zones ❑ DNS Sinkholes
ACTION	❑ Audit Logs ❑ Proxy Detection	❑ Firewall ACL ❑ Net. Segmentation ❑ Egress Filter	❑ DLP/DEP ❑ NIPS/HIPS ❑ Egress Filter	❑ Quality of Service ❑ HTTP Throttling ❑ Net. Segmentation	❑ Honeypot	❑ Trust Zones ❑ Incident Response ❑ Firewall ACLs

Fig. 3. Matrix of defensible actions at each step of an attack.

industrial networks. These solutions also fall under the categories mentioned previously; however, they are designed to be compatible with OT network protocols and standards. For example, unidirectional gateways ensure limited (if not zero) network interaction from the IT to the OT domain, and should be considered as a firewall with a very restricted communication rule consistent with the OT architecture and its security needs. Hence, this OT-specific security control is a boundary defense control (Table 1). Similarly, passive asset discovery in OT networks is a basic security control to create an inventory of authorized and unauthorized devices (Table 1, No. 1). Department of Energy (2005) lists 21 actions that can increase the security of SCADA networks. Each action corresponds to one or multiple security controls listed here.

Incidents

In this review, a cybersecurity incident refers to an incident that has been maliciously launched from cyberspace to cause adverse consequences to a target entity. All available reports on disclosed, documented, and malicious cybersecurity incidents in WWS that happened until the end of May 2019 were considered, but only incidents with detailed and verified information were selected. The information sources included reports published by government organizations, scientific papers, internal reports from affected utilities, and media coverage that reported interviews with the involved official representatives. The authors did not conduct any direct investigation themselves. The review was not restricted to any particular geographic region. All incidents, which are presented in chronological order, were true positives, with the exception of one incident. This was included due to the negative cry-wolf effects it created in the aftermath of its disclosure. For each incident, we described the situation, response/recovery (if available), and lessons learned.

Maroochy Water Services, Australia, 2000

Incident

Maroochy Shire is located about 100 km north of Brisbane in the Sunshine Coast region of Queensland, Australia. It has a population of nearly 120,000 inhabitants and a gravity sewage collection and treatment system that processes an average of 35 million L sewage each day. During the period 1997–2000, Hunter Watertech (HWT, Blackburn, Australia), a third-party contractor, installed PDS Compact 500 (Hunter Watertech, Blackburn, Australia) RTUs at all 142 sewage pumping stations. This enabled remote control and monitoring of the pumps through a SCADA system. In late January 2000, the SCADA started experiencing faults, such as loss of communication and pump control capabilities, false alarms, and altered configuration of the pumping stations. The incident resulted in the release of nearly 1 million L raw sewage into the river, local parks, and residential grounds. About 500 m of open drain in a residential area were polluted.

Response and Lessons Learned

In March 2000, after monitoring and recording all signals, the investigators concluded that the faults were caused by a human intervention. A suspect was caught on April 23, 2000, having in his possession a PDS Compact 500 RTU, a two-way radio, a laptop, a transformer, and cables. The suspect had served as a site supervisor for Hunter Watertech until resigning due to unspecified disagreements (effective as of December 3, 1999). He was sentenced to 2 years in jail and ordered to pay AU$13,111 to the Council for the damage caused by the spill. The sewage spill and its impacts were cleaned up. The process took days and required the deployment of substantial resources.

The main hazard involved in this incident was the unauthorized access to the SCADA system, which enabled the malevolent actor to release raw sewage into the surrounding environment. No cybersecurity procedures, policies, or defenses were present, and the service contract was deficient or inadequate in its handling of the contractor's responsibilities. Because the attacker was a former supervisor of the whole project, which controlled all pumping stations, the scale of the impacts could have been more extensive. The attacker was indeed a skillful, insider adversary with an intimate knowledge of the target system. The adoption of the NIST SP 800-53 control protocols (Bodeau and Graubart 2013) would have arguably prevented all of the attacker's malicious activities. A former employee's access to the network, for example, should be terminated immediately. [The sources used herein for this incident included District Court at Maroochydore (2002), Abrams and Weiss (2008), and Sayfayn and Madnick (2017).]

Pennsylvania Water Filtering Plant, US, 2006

Incident

The Federal Bureau of Investigation (FBI) suspected a security breach at a water treatment facility in Harrisburg, Pennsylvania, in 2006. Specifically, it appeared that hackers planted a computer virus on the laptop computer of an employee. The hackers then used the infected laptop as an entry point, and installed a malicious software on the plant's computer system. The hackers were reportedly operating outside the US. The investigations further reported that the hackers did not appear to target the actual plant, but merely intended to use the computer to distribute emails and other information. It was reported that the attack nevertheless could have affected the normal operations of the plant. For example, it could have altered the concentration levels of disinfectants in the potable water.

Response and Lessons Learned

The water utility eliminated remote access to the plant and changed all passwords. In the case of this specific attack, the entry point to the plant's computer system was an employee's laptop. Such weak links should always be avoided in the security chain. Due to the distributed nature of water infrastructure, staff often resort to remote access to connect to key components and check system variables, such as tank water levels. Separating SCADA systems from administrative networks, which are connected to the internet, can decrease the risk of adversary penetrations. [The sources used herein for this incident included McMillan (2006), USEPA (2008), McGurk (2008), and RISI (2019).]

Tehama-Colusa Canal, US, 2007

Incident

The Tehama-Colusa Canal Authority (TCAA) consists of 17 water contractors of the Central Valley Project. Its service area spans across the west side of the Sacramento Valley, California. TCAA operated two canals in 2007—the Tehama Colusa Canal and the Corning Canal—that provide water for irrigation to a variety of permanent and annual crops on local farms. Both canals are owned by the federal government. In 2007, a former electrical supervisor at the TCCA was alleged to have accessed and damaged the computer used to divert water from the Sacramento River to the local farms. Fortunately, the canals still could be operated manually. In his role with TCCA, the employee was responsible for the computer systems.

Response and Lessons Learned

The employee accessed the computer system on August 15, 2007, and installed unauthorized software on the SCADA system. He was an electrical supervisor with the authority and was responsible for computer systems. The intrusion cost the TCAA more than $5,000 in damages. The employee eventually was charged with unauthorized software installation and computer damage to divert water from the Sacramento River and sentenced to 10 years imprisonment and a fine.

This incident is another case of insider attack. In this case, however, the insider reportedly still was an active employee of the affected entity at the time of the attack. [The sources used herein for this incident included McMillan (2007), Weiss (2010), and RISI (2019).]

Illinois Water Plant Pump Station, US, 2011 (False Alarm Incident)

Incident

In 2011, a pump burnout at an Illinois water plant was reported to be the result of a cyberattack. News of the suspected attack became public after a security expert obtained a report collected by the Illinois Statewide Terrorism and Intelligence Center. According to the report, a plant's employee noticed problems in the SCADA. In particular, the pump kept turning on and off and eventually burned out. The suspicions were raised in part due to the apparent connections to foreign IP addresses in the log files. This news was circulated rapidly by several credible news agencies.

Response and Lessons Learned

The FBI and DHS launched an investigation. A DHS spokesperson subsequently advised that "at this time there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety" (Zetter 2011). According to the DHS, the pump had malfunctioned multiple times during recent years. Additionally, a contractor with remote access to the computer system was on a personal trip in Russia. Investigation of the log files and interviews with the personnel collectively concluded that the reported attack was a false alarm.

Interestingly, this false alarm was circulated extensively by some credible news agencies, such as the *Washington Post*, causing anxiety and cry-wolf effects. The issue could have been prevented through a more timely consideration of the employee's international travel and the pump's malfunctioning history. Another factor that likely contributed to the cry-wolf effect was the public availability of a preliminary report that anticipated the official conclusion of the investigations. [The sources used herein for this incident included Nakashima (2011), Zetter (2011), and Parish (2011).]

Key Largo Wastewater Treatment District, US, 2012

Incident

In 2012, the former Chief Financial Officer (CFO) of Florida's Key Largo Wastewater Treatment District illegally accessed the district's computer system to download emails and other personal documents. He performed these actions using the credentials of other employees after the district did not renew his contract. He was arrested on felony charges, including computer crime with intent to defraud, modify information without authority, and delete information from the district's computer system.

Response and Lessons Learned

The facility's IT manager discovered emails addressed to the CFO's personal email account during a routine check of the email system. These emails were sent when the CFO still was working at the facility but already had been informed that his contract was not going to be renewed. Upon discovery, the IT manager informed the police, who then proceeded to arrest the CFO. The attack was limited to the IT systems of the facility, with no other malicious activity or disruptions for the district's operations.

It still is not clear how the CFO gained the credentials of his fellow employees. It is important for employees to constantly update their passwords in order to reduce the risks associated with stolen credentials. The CFO used these credentials to access the system from home, suggesting that no second authentication factor was needed to access the computer systems. Similarly to the Kemuri Water Company incident (Incident 8), a two-factor authentication could have prevented this attack. The attack was discovered through routine checks, which always should be performed extensively for systems containing sensitive and confidential data. [The sources used herein for this incident included Goverment Technology (2012) and Department of Homeland Security (2012)].

Bowman Avenue Dam, US, 2013

Incident

The Bowman Avenue Dam is a small hydraulic infrastructure used to control floods in Blind Brook Creek (Rye, New York). A key component of the dam is a remotely controllable sluice gate, in operation since 2013, that controls the water flow as a function of water levels and temperatures in the creek. Between August 28 and September 18, 2013, hackers obtained unauthorized remote access to the SCADA system, a cyberattack that allowed them to gather information on water levels, temperature, and the status of the sluice gate. The gate was manually disconnected for maintenance at the time of the intrusion, so the hackers did not have the opportunity to take direct control of the sluice gate. The attack was perpetrated with the aid of Google dorking, a computer hacking technique that leverages the Google search engine to locate specific strings—and thereby vulnerabilities—in web applications, such as the one used to monitor and control the sluice gate. The hackers' action should not be classified as an intrusion, but rather as reconnaissance, namely the first stage of the CKC [Fig. 2(a)], in which the attacker gathers information on a potential target by looking for publicly available information on the internet. The attackers used a standalone PC of the dam's system to access its control network. However, at the time of attack, the control system was only gathering water level information and storing it in a spreadsheet. The control system was connected to the internet through a cellular mode. Despite being accessible directly through the internet, it was not safeguarded by reliable security measures such as firefall or authentication access controls.

Response and Lessons Learned

Since the attack, a new software application and a new sluice gate have been installed. At Governor Cuomo's direction, New York State has taken multiple steps to improve its cybersecurity capabilities across several sectors. The investigations carried out by the DHS and the Justice Department resulted in the indictment of a few state-sponsored hackers. The attack caused over $30,000 in remediation costs. Although this attack had no consequences for the security and reliability of the Bowman Avenue Dam, it points to the vulnerabilities of critical water infrastructures, which often are monitored and controlled through unsafe web applications. It thus is not completely surprising to observe that the attack happened only 2 months after the intallation of an unsafe web application. [The sources used herein for this incident included Cuomo (2016), Lach (2016), Kutner (2016), and Lund et al. (2019).]

Five Water Utilities, US, 2014

Incident

In the spring of 2014, five water utilities across three states in the US experienced some problems with their smart water meters. In particular, they faced inaccurate water bills and the deactivation of the tower gateway base stations (TGBs), which receive signals from the water meters and transfer them to centralized facilities for monitoring and billing purposes. The first incident was reported by Kennebec Water District (Maine), in which the utility could not connect to the TGB. Nine other attacks were reported in Spotswood (New Jersey), Egg Harbor (New Jersey), Aliquippa (Pennsylvania), and New Kensington (Pennsylvania).

The attack was caused by a fired employee of the company that manufactured the smart water meters—named Company A in court documents—who gained unauthorized access to protected computers. Specifically, the employee had worked as a field radio frequency engineer and was fired in November 2013. A few weeks later, using his access to the base station network, he conducted various malicious activities, such as changing the root passwords, modifying the TGB radio frequency, and overwriting computer scripts.

Response and Lessons Learned

This abnormality drew the attention of the Federal government and caused investigations of possible cyberattacks against the water infrastructures. Because the attack disabled the communication between utilities and their data collection network, the organizations had to resume manual data gathering. In addition, Company A had to carry out forensic investigations at its own expense to identify the attacker, characterize the attacks, and find and repair the damage.

Although the utilities suspected that the disgruntled employee could have accessed the systems before May 2014, investigators could not link some anomalies to the attacker, because login details were not recorded at that time. However, recorded logins showed multiple intrusions linked to the IP address of the attacker's home. The attacker was indicted for several malicious activities, and sentenced to prison and the payment of a fine.

Although the attacker was not a professional hacker, a default password allowed him to access the TGB. This highlights the importance of implementing access control and revoking access rights when someone is laid off. In addition, it is important to log and store in a safe place all logins and user's activities. If Company A had kept track of logins earlier, investigators could have discovered breaches from prior to May 2014. This would have helped the investigations. [The sources used herein for this incident included Department of Justice (2017), Cimpanu (2017), Vaas (2017), and Gallagher (2017).]

Kemuri Water Company (Pseudonym), US, 2016

Incident

In 2016, an undisclosed water utility in the US (presented under the pseudonym of Kemuri Water Company) hired Verizon Security Solutions to perform a proactive cybersecurity assessment of its water supply and metering system. A comprehensive assessment was subsequently conducted on both its OT (distribution, control, and metering) and IT (personal and billing information of the customers) systems. The assessment revealed several high-risk vulnerabilities, including a heavy reliance on outdated computers and operating systems. This included an outdated midrange computer system (AS400, IBM, Armonk, New York) system that served a number of critical OT and IT functions—including the utility's valve and flow control application—and had direct connections to many networks.

The detection of these vulnerabilities triggered a full response and investigation. A cross-correlation of the utility's internet traffic against a repository of known threat actors disclosed a positive match with the IP addresses of state-sponsored hacktivists. Interviews were conducted with the utility's staff, which revealed that some staff members were aware of possible unauthorized access to the systems as well as a series of unexplained valve manipulation patterns. This casts doubt on whether the call for a forensic investigation was proactive, rather than reactive.

A physical survey revealed the presence of a wired connection between the utility's internet payment application and the AS400 system. Because the AS400 was open to the internet, it was concluded that access to the payment application also would have granted access to any information stored in the AS400. Collectively, the forensic investigations discovered an actual exploitation of the internet-facing payment application server and the subsequent manipulation of the utility's valve and flow control application. The incident resulted in the exfiltration of 2.5 million unique records and manipulation of chemicals and flow rates.

Response and Lessons Learned

Access to and from the account management web front was terminated, and outbound connectivity of the AS400 system was blocked immediately. Recommendations were made to replace the antiquated systems with more-modern versions.

Multiple exploitable vulnerabilities led to the breach, which could have led to more serious consequences if the forensic investigation had not been conducted or the attackers had more knowledge of the utility's OT and IT systems. Internet-facing servers and applications, such as the payment management application in this case, should not be connected to the SCADA. The utility had relied on a single-factor authentication; this is not sufficient, and multifactor authentication should be used. Outdated systems, such as the AS400 in this case, which formed a single point of failure, should not be deployed, and installation of security patches should not be overlooked. Exfiltration of records went unnoticed for a long time and in large amounts. A monitoring mechanism should be in place to oversee the transfer of data and to enable early detection and response. [The sources used herein for this incident included Verizon (2016) and Mahairas and Beshar (2018).]

Undisclosed Utility, US, 2016

Incident

In 2016, the system administrator of a small water utility noticed the emergence of suspicious network traffic data. In particular, the administrator found heavy network traffic originating from the control panel of a pumping station. This triggered the possibility of a cyberattack and a subsequent call to ICS-CERT. An official investigation was promptly launched.

Response and Lessons Learned

The ICS-CERT was immediately provided with the data on the network configuration. Address white lists were instituted. Together with a transition to nonstandard ports, these actions enabled safeguarding the network without requiring that the control interface be put in offline mode. Within a few days, ICS-CERT also collected forensic images of the network hardware. Reverse engineering of the malware subsequently was performed to determine the attacker, breach point, data compromised, and mitigation strategy to prevent the same attack at other facilities. No details of the key findings have been disclosed.

The situational awareness of the system administrator and prompt notification of ICS-CERT proved to be effective in isolating and thwarting a potentially catastrophic intrusion. Under the Critical Infrastructure Information Act of 2002 (CII Act), the DHS has established the Protected Critical Infrastructure Information (PCII) Program to assure utilities that their submitted information will not be disclosed. [The source used herein for this incident is ICS-CERT (2016a).]

Undisclosed Drinking Water Utility, US, 2016

Incident

In late 2016, an American water authority noticed a 15,000% increase in their monthly cellular data bills. The authority was hacked between November 2016 and January 2017. The utility had seven Sixnet BT (Red Lion, York, Pennsylvania) series cellular routers, which provided wireless access for monitoring the utility's pumping stations as well as a few other sites. Four of these seven routers were compromised by hackers. The hack was believed to be an opportunistic action to steal valuable internet bandwidth, resulting in the authority's cellular data bill soaring from an average of $300 a month to $45,000 in December 2016 and $53,000 in January 2017. However, the intrusion did not damage the utility's infrastructure and did not cause any physical harm. The cause of the attack may stand in the Sixnet BT series hard-coded credentials vulnerability (identified by the DHS in May 2016). A poorly skilled hacker should be able to exploit this vulnerability by hacking a factory-installed password. Sixnet (Red Lion, York, Pennsylvania) produced patches and new firmware to mitigate this vulnerability.

Response and Lessons Learned

The use of hard-coded credentials by the router manufacturer and the failure of the water authority to install the patches proved to be major contributors to this incident. [The sources used herein for this incident included Walton (2017) and Jerome (2017).]

Regional Water Supplier, UK, 2017

Incident

A regional water supplier was notified by several of its clients that their online account details were changed. After the clients credential were reset, it emerged that the details of some registered bank accounts also were changed, so that refunds issued to the customers were transferred fraudulently to these new bank accounts. The diverted refunds totaled over £500,000 and were directed to two bank accounts in England. The banks holding these accounts were socially engineered and allowed the holders to quickly transfer the majority of the funds to other bank accounts in Dubai and the Bahamas. Subsequently, these funds were used to purchase Bitcoins, which were then transferred to addresses associated with a Bitcoin mixing service, thus preventing any subject to be identified by following this trail further.

Response and Lessons Learned

The company initially notified its legal advisor about the data breach. When the efforts to track down the bank account holders failed, the legal advisor contacted Verizon's cybersecurity experts, who started investigating within the company's premises. The experts proceeded to analyze the systems and processes involved in managing the customers' accounts. After a due-diligence review of logs and web servers revealed that no malicious software was present, the Verizon team suggested interviewing personnel involved with customers' accounts. The interviews were extended to various stakeholders, including a third-party call center in Mumbai (India), which was responsible for administering the online accounts and processing telephone payments. After reviewing the customer relationship management's log files, the investigators were able to confirm that one employee had accessed all the accounts that were fraudulently refunded. In-depth analysis of the employee's computers revealed that, despite the use of data-wiping software, he had sent numerous email messages concerning the accounts affected by the fraudulent activity to another individual based in England. When presented with this evidence, the suspected worker finally confessed to the crime and offered assistance in identifying accounts with over £1,000 in refunds stolen. The employee took photographs of the account details and sent them to his aide in England, who then created an online account or requested a password reset. With the help of the call center employee, new evidence was gathered, and authorities also were able to secure a conviction for the aide.

This insider attack suggests that management also should ensure that partners with access to critical data perform stringent background checks on their employees. [The source used herein for this incident was Verizon (2017).]

European Water Utility, 2018

Incident

A European water utility with a cloud-based OT analytics system hired a critical infrastructure security firm, Radiflow, to monitor its network. On January 21, 2018, suspicious network traffic was detected on the SCADA network. A series of new links to external IP addresses created a major network topology change, which triggered several alerts. The destination IP addresses were looked up, but this did not lead to any malicious site. Further investigation revealed that the addresses belonged to MinerCircle Monero Pool. This led to the detection of cryptomining malware in the OT network of the water utility. The investigation classified nearly 40% of the traffic as related to mining operations, causing a 60% surge in the overall bandwidth consumption. The investigation found no attempts to manipulate the controller configuration or send commands.

Response and Lessons Learned

The security firm informed the water utility of the cryptomining malware and infected servers. The recovery scheme included updating the antivirus software on some servers as well as tightening the firewall security. The updated antivirus software was successful in detecting the CoinMiner malware.

This incident is believed to be the first known instance of cryptojacking—i.e., the unauthorized use of a computing resource to illicitly mine cryptocurrency—being used against an ICS. Suspicious network traffic was the clue that led to the detection of the cryptojacking in this incident. In addition to suspicious network traffic, high processor usage, sluggish response times, and overheating are some symptoms of cryptojacking that can be monitored for early detection. [The sources used herein for this incident included Radiflow (2018), Newman (2018), and Kerner (2018).]

Onslow Water and Sewer Authority, US, 2018

Incident

Onslow Water and Sewer Authority, a water utility company in Jacksonville (North Carolina) was targeted by cybercriminals in October, 2018. Beginning immediately in the wake of Hurricane Florence, the attack soon escalated into a sophisticated ransomware attack that locked out employees and encrypted databases, leaving the utility with limited computing capabilities. The hack began with persistent cyberattacks through a virus known as EMOTET. With the EMOTET virus infection persisting, the authority reached out to outside security experts to investigate and respond to the attack. At approximately 3 a.m. on Saturday, October 13, while the investigations were still underway, the malware launched a more sophisticated virus known as RYUK. The IT team immediately disconnected the authority's facilities from the internet. Nevertheless, the situation soon exacerbated and the virus encrypted files and data. The authority suspects this was a targeted attack, because the hackers chose a target that recently had been hit by a natural disaster. Moreover, the sophisticated virus was launched at 3 a.m. on a Saturday—a time at which the authority was most vulnerable. The authority soon received one email from the cyber criminals demanding payment to decrypt the damaged files and data. The authority dismissed the offer and stated that it will not "negotiate with criminals nor bow to their demands" (Gray 2018).

Response and Lessons Learned

The authority has been working with the FBI, the DHS, the state of North Carolina, and multiple security firms for remediation and recovery. The authority also planned to rebuild its IT systems from the ground up.

The authority had multiple layers of protection in place, including firewalls and antivirus/malware software, when the hackers struck. However, their IT system proved to be penetrable. Ransomware is the fastest-growing malware threat, targeting users of all types, according to the FBI. In this incident, the utility decided not to pay a ransom. This is in accordance with the federal guidelines—the US Government does not encourage paying a ransom to criminal actors. [The sources used herein for this incident included ONWASA (2018) and Mahairas and Beshar (2018).]

Fort Collins Loveland Water District, US, 2019

Incident

Fort Collins Loveland Water District serves customers in parts of Fort Collins, Loveland, Timnath, Windsor, and Larimer County (Colorado). On February 11, 2019, the staff of the Fort Collins Loveland Water District and South Fort Collins Sanitation District were unable to access technical data. Daily operations and customer data were not believed to have been compromised. The utility had fallen victim to a ransomware cyberattack. The hackers demanded a ransom to restore access (the amount of ransom payment demanded has not been disclosed to the public). The district declined to pay the ransom.

Response and Lessons Learned

Within a few weeks, the district managed to unlock the data on its own. The decision about whether or not to notify the customers about the hack was also a challenge. Eventually, it was decided not to notify them, because the district did not store customers' data. All payments were handled by a third-party vendor.

This is another case of a ransomware attack in which the victim declined to pay a ransom. Data segmentation and segregation proved to be a helpful practice in safeguarding sensitive customer and daily operation data. Hiring a third-party vendor to handle customer payments prevented the customer data from being compromised. The practice of hiring third-party vendors, however, creates its own risks, as in Incident 11. [The sources used herein for this incident included Ferrier (2019) and Sobczak (2019).]

Riviera Beach Water Utility, US, 2019

Incident

On May 29, 2019, Riviera Beach, a small city of 35,000 inhabitants located north of West Palm Beach (Florida), was hit by a crippling ransomware attack after an employee of the police department opened an infected email. Paralyzing computer systems of the police department, city council, and other local government offices, the ransomware sent all operations offline and encrypted their data. The attack also spread to the water utility, compromising the computer systems controlling pumping stations and water quality testing, as well as its payment operations.

Response and Lessons Learned

A few days after the attack, the city council unanimously voted to authorize its insurer to pay 65 bitcoins, approximately $600,000, to the attackers. The city would pay an additional $25,000 as insurance deductibles out of its budget. Two weeks after the attack was disclosed, the IT department made the city's website and email services fully operational, although the water pump stations and water quality testing systems were only partially available. Although water quality sampling had to be performed manually, the city council's spokeswoman assured that water quality itself was never in jeopardy. The FBI, Secret Service, and DHS investigated the attack and recommended that the city not pay the ransom. Although the ransom was paid, as of June 20, 2019, the sensitive data encrypted by the hackers still were inaccessible.

While waiting for the attackers to share a decryption key, the local government authorized spending more than $900,000 to buy new computer hardware—purchases which were planned for the following year. According to a councilperson, most of the existing hardware was old and outdated, which made it vulnerable to the cyberattack. In addition, the city's computer network was not updated, and patches were not installed on time.

It is known that local governments and small public utilities are less prepared for cyberattacks, because they lack the budget and professionals needed to secure their IT and OT systems. However, basic cybersecurity training raises awareness and reduces the possibility of succumbing to devastating attacks unleashed by the naivety of uninformed employees, such as in the case of Riviera Beach. Although paying a ransom seems to be the easiest way to solve the problem, the FBI and security experts suggest never paying a ransom, because it only encourages future criminal activity. Preventing cyberattacks from happening is always the best practice. [The sources used herein for this incident included Doris (2019), Mazzei (2019), and O'Donnell (2019).]

Discussion

As outlined in the previous section, the complexity of cyberincidents in WWS has increased during the last two decades. In some earlier incidents, such as the 2000 Maroochy Water Services hack, an insider simply and directly gained access to the OT controllers and performed malicious activities, whereas in some recent attacks, such as the 2016 Kemuri Water Company hack, several IT and OT workstations were compromised by outsiders using multistep attack techniques. This section reviews and analyzes some key points of the aforementioned incidents from both attacker and defender's perspectives.

Table 2 provides an overview of the time, location, targeted systems type, investigation teams (i.e., target organization, third-party security teams, or governmental agencies), and impacts associated with each incident. The majority of targeted systems were US-based water systems, which might be because (1) they use more-advanced networking technologies (integrated IT/OT architecture) and thus are more exposed to the internet; (2) they are lucrative targets for hackers with a wide variety of goals; and (3) incident reporting and information sharing is more systematically and extensively encouraged, required, and pursued in the US (NIST 2012). There have been claims of WWS cyberattacks in other countries, such as Ukraine (Martin 2018), but limited reliable information is publicly available for such incidents. The WWS systems targeted by the cybercriminals have been very diverse, ranging from water supply systems to wastewater treatment plants, underlining the fact that all types of water systems are susceptible to cyberattacks. Table 2 also indicates that the consequences of the cyberattacks have been extremely diverse. The attacks have led to the pollution of open water bodies, theft of irrigation water, data breaches, and manipulation of chemical rates in potable water, to name a few. No reports of human casualties were found by this study. Furthermore, the primary incident investigators rarely come from the victim's organization. This might indicate a shortage of in-house security teams or trained personnel.

Attackers usually are grouped based on their capabilities, motivations, and goals. Based on these characteristics, various groups of attackers are defined, such as script kiddies (SKs) (curious, unskilled individuals), cyberterrorists (physical damage goals), cybercriminals (financial goals), hacktivists (social or political goals), and state-sponsored actors. Some other groups, such as cyber researchers, white/black hats, and internal actors, also have been proposed in the literature (Ablon 2018). Regardless of their goals and capabilities, attackers can be insiders or outsiders. Table 3 summarizes the type of attackers, their target assets and domains, and their final actions against the observed targets. The attacker and group for Incident 4 are not available simply because the incident was later confirmed to be a false alarm. Insiders are common adversaries in the water sector, as reported for the Key Largo Wastewater Treatment District, Maroochy Shire, Tehama Colusa Canal Authority, the five Eastern water utilities attacks, and a regional water supplier hack (Incidents 1, 3, 5, 7, and 11). This suggests that management and security teams should be more cognizant of changes in the behaviors of employees. For example, in the Maroochy Water

Table 2. Summary of incidents

Number	Location	Year	Target system	Investigator	Primary impact
1	Australia	2000	Wastewater	HWT and Queensland EPA	Environmental pollution
2	Pennsylvania	2006	Water treatment	FBI	Data breach
3	California	2007	Irrigation	System personnel	Water theft
4	Illinois	2011	Water plant	DHS	Cry-wolf effects
5	Florida	2012	Wastewater	System personnel	Data breach
6	New York	2013	Dam	Justice department	Data breach
7	US	2013	Water utility	Third-party provider	Data manipulation
8	US	2016	Water utility	Verizon security	Control manipulation
9	US	2016	Water utility	DHS	Data breach
10	US	2016	Water utility	DHS	Bandwidth theft
11	UK	2017	Water supplier	Verizon security	Financial impact
12	Europe	2018	Water utility	Radiflow	Resource theft
13	North Carolina	2018	Water utility	State and Federal	Data loss
14	Colorado	2019	Water district	System personnel	Denial of access
15	Florida	2019	Water utility	FBI, DHS and Secret Services	Data loss

Table 3. Adversary analysis

Number	Attacker	Group	Target	Domain	Action
1	Insider	Internal actor	RTU/PLC	OT	Configuration change
2	Outsider	SK	Workstations	IT	Data exfiltration
3	Insider	Internal actor	SCADA	OT	Software installation
4	N/A	N/A	SCADA	OT	Physical process issue
5	Insider	Cybercriminal	Mail/file server	IT	Data exfiltration
6	Outsider	State-sponsored	SCADA/HMI	OT	Data exfiltration
7	Insider	Cybercriminal	Multiple	IT and OT	Unauthorized changes
8	Outsider	State-sponsored	Multiple	IT and OT	Multiple
9	Unknown	Unknown	SCADA	OT	Data exfiltration
10	Unknown	SK	Routers	OT	Unauthorized access
11	Insider	Cybercriminal	Account database	IT	Unauthorized access
12	Outsider	Cybercriminal	SCADA/HMI	OT	Cryptojacking
13	Outsider	Cybercriminal	SCADA/HMI	OT	Cryptojacking
14	Outsider	Cybercriminal	Info. system	IT	Ransomware
15	Outsider	Cybercriminal	Databases	IT and OT	Ransomware

attack, the attacker was no longer an employee. However, he still had access to the wireless network. Thus, he can be considered as an insider causing physical and financial damages (both cybercriminal and cyberterrorist). In some similar examples, such as Incidents 3, 5, and 7, former employees or contractors tried to cause harm (financially or physically) through an unauthorized access to the IT or OT systems. In case of Incident 7, the attacker chose multiple targets in different domains of five utilities.

The attacker in the second incident most likely was a script kiddie outsider who installed malware on the victim's computer to gain access to the internal information and distribute emails and information—there is no evidence of other groups of attackers in the public report. However, it is known that Attack 8 was performed by state-sponsored parties who targeted multiple IT and OT systems that resulted in the data exfiltration and manipulation of chemical and flow rates. Incident 4 is known as a false alarm; however, several operational issues were observed at the same time, thereby confusing the investigation team. Recent incidents (since 2017) appear to have a more complex nature (Table 3). The attackers, insiders or outsiders, have been targeting databases, files, and account servers of the victims for financial purposes. As organizations advance and integrate their IT and OT systems and limit the OT systems from accessing to internet directly, the IT systems become of more interest for attackers and the entry point to the victim's network. The most interesting and unusual attack in this study is perhaps Incident 12, in which attackers deployed a cryptocurrency mining code on the OT network of the target utility (most likely downloaded from malicious websites) to use the computational resources of OT machines as part of a mining pool that creates or discovers digital currency.

No single defense mechanism can protect WWS against cyberthreats, so defense teams should use any mechanism (e.g., detect, deny, or deceive) offered by critical security controls (CSC) (CIS 2019) (Table 1). Table 4 outlines the most needed protection mechanisms and the three most basic and foundational CSCs for the attacks described in this study. The foundational CSCs are associated with specific architectural levels, based on the attacker's first step and weakest point of the victim's network. In almost all incidents, there was a lack of organizational controls, such as security skills assessment and appropriate training to fill gaps or incident response and management. Although many organizations use proactive approaches—such as routine vulnerability and threat assessment or adversary simulation (i.e., red teaming, CSC 20)—to find security flaws in their network, most of the reviewed incidents were not detected proactively. A reactive security strategy, as seen in most industrial networks triggers, is to respond when something happens. Table 4 also shows that most WWS networks suffer from a lack of preventive security mechanisms (Fig. 3, column Deny), that is, the first line of defense in cybersecurity practice.

Table 4. Defense analysis

Number	Approach	Protection	Basic CSC	Foundational CSC	Architectural level
1	Reactive	Deny	1, 3, 5	12, 15, 16	1–2
2	Reactive	Deny	2, 3, 4	7, 8, 14	2 and 4
3	Reactive	Deny	2, 3, 5	11, 14, 16	2–3
4	Reactive	Detect	2, 5, 6	9, 11, 12	2–3
5	Proactive	Deny	3, 5, 6	7, 13, 16	5 (or DMZ)
6	Unknown	Deny	2, 4, 6	9, 11,12	2–3
7	Reactive	Deny	1, 3, 5	14, 15, 16	2–4
8	Proactive	Detect	1, 3, 4	9, 11, 14	2–5
9	Reactive	Disrupt	2, 3, 4	8, 9, 13	2–3
10	Reactive	Deny	3, 4, 5	11, 14, 15	3–5
11	Reactive	Degrade	4, 5, 6	12, 13, 14	4–5
12	Proactive	Deny	2, 3, 4	7, 8, 11	2–3
13	Reactive	Contain	2, 3, 4	8, 10, 13	4–5
14	Reactive	Contain	2, 3, 4	8, 10, 13	3–5
15	Reactive	Contain	2, 3, 4	7, 8, 10	3–5

Epilogue

This study presented a review of 15 cybersecurity incidents in the water and wastewater sector within the context of industrial network architectures and attack-defense models. The incidents covered a wide variety of vulnerabilities and situations. The incidents spanned over 18 years, from the Maroochy Shire Sewage Treatment Plant insider attack in 2000 to the Riviera Beach Water Utility ransomware attack in 2019. This review is an informative resource to guide securing of industrial control systems in WWS and other lifeline sectors against cyberthreats. The sheer diversity of the systems, attackers, and consequences associated with the incidents dictate a need for inclusive and comprehensive vulnerability assessments, as well as risk mitigation, preparedness, response, and recovery studies that account for such extreme heterogeneity.

Because the reports by official agencies indicated a large number of cybersecurity incidents in the WWS, this review may not be inclusive of all incidents. Many of them may not be made public. The framework developed by this study, however, was structured and designed so that it can readily accommodate extensions and updates as more incidents are possibly disclosed (or take place in the future). The development and maintenance of an online version of this repository is believed to be a significant future endeavor to pursue.

Data Availability Statement

No data, models, or code were generated or used during the study.

Acknowledgments

Mohsen Aghashahi and M. Katherine Banks are supported by Qatar National Research Fund (QNRF) under Grant NPRP8-1292-2-548. Riccardo Taormina and Stefano Galelli are supported in part by the National Research Foundation (NRF) of Singapore under its National Cybersecurity R&D Programme (Award no. NRF2014NCR-NCR001-40). Avi Ostfeld is supported by the EU H2020 STOP-IT project (Grant agreement 740610).

References

Ablon, L. 2018. "Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data." Accessed August 15, 2019. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf.

Abrams, M., and J. Weiss. 2008. *Malicious control system cyber security attack case study–Maroochy Water Services, Australia*. McLean, VA: The MITRE Corporation.

Ahmed, C. M., C. Murguia, and J. Ruths. 2017. "Model-based attack detection scheme for smart water distribution networks." In *Proc., 2017 ACM on Asia Conf. on Computer and Communications Security*, 101–113. New York: Association for Computing Machinery.

Amin, S., X. Litrico, S. Sastry, and A. M. Bayen. 2013. "Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks." *IEEE Trans. Control Syst. Technol.* 21 (5): 1963–1970. https://doi.org/10.1109/TCST.2012.2211873.

Bodeau, D., and R. Graubart. 2013. *Cyber resiliency and NIST special publication 800-53 rev. 4 controls*. MITRE Technical Report. McLean, VA: MITRE Corporation.

Bodeau, D., R. Graubart, and W. Heinbockel. 2013. *Characterizing effects on the cyber adversary.* MTR130432. McLean, VA: MITRE Corporation.

Caltagirone, S., A. Pendergast, and C. Betz. 2013. *Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data*. Hanover, MD: Center for Cyber Intelligence Analysis and Threat Research.

Cava, M. D. 2018. "Uber to pay $148 million over undisclosed data breach that ex-CEO paid hackers to keep quiet." Accessed August 15, 2019. https://www.usatoday.com/story/tech/news/2018/09/26/uber-pay-148-million-over-undisclosed-data-breach-ex-ceo-paid-hackers-keep-quiet/1432335002.

Chandy, S. E., A. Rasekh, Z. A. Barker, and M. E. Shafiee. 2018. "Cyberattack detection using deep generative models with variational inference." *J. Water Resour. Plann. Manage.* 145 (2): 04018093. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001007.

Cimpanu, C. 2017. "Fired employee hacks and shuts down smart water readers in five US cities." Accessed August 15, 2019. https://www.bleepingcomputer.com/news/security/fired-employee-hacks-and-shuts-down-smart-water-readers-in-five-us-cities/.

CIS (Center for Internet Security). 2019. "CIS controls." Accessed August 15, 2019. https://www.cisecurity.org/controls.

Cuomo, A. 2016. "Statement from Governor Andrew M. Cuomo on cyber attack charges announced by U.S. Attorney General Loretta Lynch and FBI Director James Comey Involving the Bowman Avenue Dam in Westchester County." Accessed August 15, 2019. https://www.governor.ny.gov/news/statement-governor-andrew-m-cuomo-cyber-attack-charges-announced-us-attorney-general-loretta.

Department of Energy. 2005. "21 steps to improve cyber security of SCADA network." Accessed August 15, 2019. https://www.hsdl.org/?abstract&did=1826.

Department of Homeland Security. 2012. "Daily open source infrastructure report 27 March 2012." Accessed February 11, 2020. https://www.dhs.gov/xlibrary/assets/DHS_Daily_Report_2012-03-27.pdf.

Department of Justice. 2017. "Bala Cynwyd man sentenced to prison for hacking computers of public utilities." Accessed August 15, 2019. https://www.justice.gov/usao-edpa/pr/bala-cynwyd-man-sentenced-prison-hacking-computers-public-utilities.

District Court at Maroochydore. 2002. "Appeal against conviction and sentence proceedings regarding appellant Vitek Boden." Accessed August 15, 2019. https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf.

Doris, T. 2019. "Why Riviera Beach agreed to pay a $600,000 ransom payment to regain data access . . . and will it work?" Accessed August 15, 2019. https://www.palmbeachpost.com/news/20190619/why-riviera-beach-agreed-to-pay-600000-ransom-payment-to-regain-data-access-and-will-it-work.

Ferrier, P. 2019. "Cyberattacker demands ransom from Northern Colorado utility." Accessed August 15, 2019. https://www.coloradoan.com/story/money/2019/03/14/cyberattacker-demands-ransom-colorado-utility/3148951002.

Formby, D., S. Durbha, and R. Beyah. 2017. "Out of control: Ransomware for industrial control systems." In *Proc., RSA Conf.* Bedford, MA: RSA Security.

Gallagher, S. 2017. "Some beers, anger at former employer, and root access add up to a year in prison." Accessed August 15, 2019. https://arstechnica.com/information-technology/2017/06/ex-technician-convicted-of-possibly-drunken-attack-on-smart-water-meter-system.

Government Technology. 2012. "Report: Hacking lands Florida wastewater official in hot water." Accessed August 15, 2019. https://www.govtech.com/public-safety/Report-Hacking-Lands-Florida-Wastewater-Official-in-Hot-Water.html.

Gray, P. 2018. "When it comes to ransomware demands, just say no." Symantec. Accessed February 10, 2020. https://www.symantec.com/blogs/feature-stories/when-it-comes-ransomware-demands-just-say-no.

Hassanzadeh, A., and R. Burkett. 2018. "SAMIIT: Spiral attack model in IIOT mapping security alerts to attack life cycle phases." In *Proc., 2018 Int. Symp. for ICS and SCADA Cyber Security Research (ICS-CSR 2018)*, 11–20. London: British Computer Society.

Hassanzadeh, A., S. Modi, and S. Mulchandani. 2015. "Towards effective security control assignment in the industrial internet of things." In *Proc., 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 795–800. New York: IEEE.

Housh, M., and Z. Ohar. 2018. "Model-based approach for cyber-physical attack detection in water distribution systems." *Water Res.* 139 (Aug): 132–143. https://doi.org/10.1016/j.watres.2018.03.039.

Hutchins, E. M., M. J. Cloppert, and R. M. Amin. 2011. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." In Vol. 1 of *Leading issues information warfare security research*, 187. Sonning Common, England: Academic Conferences and Publishing International Limited.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). 2016a. *ICS-CERT monitor: March/April 2016*. Washington, DC: US Dept. of Homeland Security.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). 2016b. *NCCIC/ICS-CERT year in review: FY 2015*. Washington, DC: US Dept. of Homeland Security.

ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). 2019. "DHS critical infrastructure cyber community voluntary program." Accessed August 15, 2019. https://www.cisa.gov/ccubedvp.

International Society of Automation. 2009. *Security for industrial automation and control systems*. ISA-62443. Durham, NC: International Society of Automation.

Jerome, S. 2017. "Utility cyberattack targets bandwidth, not water." Accessed August 15, 2019. https://www.wateronline.com/doc/utility-cyberattack-targets-bandwidth-not-water-0001.

Kerner, S. 2018. "Water utility in Europe hit by cryptocurrency malware mining attack." Accessed August 15, 2019. https://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack.

Krutz, R. L. 2005. *Securing SCADA systems*. Chichester, UK: Wiley.

Kutner, M. 2016. "Alleged dam hacking raises fears of cyber threats to infrastructure." Accessed August 15, 2019. https://www.newsweek.com/cyber-attack-rye-dam-iran-441940.

Lach, E. 2016. "Cyber war comes to the suburbs." Accessed August 15, 2019. https://www.newyorker.com/tech/annals-of-technology/cyber-war-comes-to-the-suburbs.

Laszka, A., W. Abbas, Y. Vorobeychik, and X. Koutsoukos. 2017. "Synergic security for smart water networks: Redundancy, diversity, and hardening." In *Proc., 3rd Int. Workshop on CyberPhysical Systems for Smart Water Networks*, 21–24. New York: Association for Computing Machinery.

Lund, P. D., J. Byrne, R. Haas, and D. Flynn, eds. 2019. *Advances in energy systems: The large-scale renewable energy integration challenge*. New York: Wiley.

Mahairas, A., and P. Beshar. 2018. "A perfect target for cybercriminals." Accessed August 15, 2019. https://www.nytimes.com/2018/11/19/opinion/water-security-vulnerability-hacking.html.

Martin, A. 2018. "Russian hackers targeted Ukraine's water supply, security service claims." Accessed August 15, 2019. https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826.

Mazzei, P. 2019. "Hit by ransomware attack, Florida city agrees to pay hackers $600,000." Accessed August 15, 2019. https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html.

McGurk, S. P. 2008. *Industrial control systems security: Protecting the critical infrastructure*. Washington, DC: US Dept. of Homeland Security.

McMillan, R. 2006. "Hackers break into water system network." Accessed August 15, 2019. https://www.computerworld.com/article/2547938/hackers-break-into-water-system-network.html.

McMillan, R. 2007. "Insider charged with hacking California canal system." Accessed August 15, 2019. https://www.computerworld.com/article/2540235/insider-charged-with-hacking-california-canal-system.html.

Nakashima, E. 2011. "Water-pump failure in Illinois wasn't a cyberattack after all." Accessed August 15, 2019. https://www.washingtonpost.com/world/national-security/water-pump-failure-in-illinois-wasnt-cyberattack-after-all/2011/11/25/gIQACgTewNstory.html.

Newman, L. 2018. "Now cryptojacking threatens critical infrastructure, too." Accessed August 15, 2019. https://www.wired.com/story/cryptojacking-critical-infrastructure.

NIST. 2012. *Computer security incident handling guide*. Washington, DC: NIST.

O'Donnell, L. 2019. "Post-ransomware attack, Florida city pays $600K." Accessed August 15, 2019. https://threatpost.com/ransomware-florida-city-pays-600k-ransom/145869.

ONWASA (Onslow Water and Sewer Authority). 2018. "Cyber-criminals target critical utility in hurricane-ravaged area." Accessed August 15, 2019. https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A.

Parish, J. 2011. "Illinois water plant 'hack' was denied by FBI and DHS and later proved a false alarm." Accessed August 15, 2019. https://www.theverge.com/2011/12/1/2604353/illinois-water-plant-hack-was-denied-by-fbi-and-dhs-and-later-proved.

Radiflow. 2018. "Detection of a crypto-mining malware attack at a water utility." Accessed August 15, 2019. https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility.

Ramotsoela, D. T., G. P. Hancke, and A. M. Abu-Mahfouz. 2019. "Attack detection in water distribution systems using machine learning." *Hum. Centric Comput. Inf. Sci.* 9 (1): 13. https://doi.org/10.1186/s13673-019-0175-8.

Rasekh, A., A. Hassanzadeh, S. Mulchandani, S. Modi, and M. K. Banks. 2016. "Smart water networks and cyber security." *J. Water Resour. Plann. Manage.* 142 (7): 01816004. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000646.

RISI (Repository of Industrial Security Incidents). 2019. "The Repository of Industrial Security Incidents." Accessed August 15, 2019. https://www.risidata.com.

Rubin, G. T. 2019. "Many company hacks go undisclosed to SEC despite regulator efforts." Accessed August 15, 2019. https://www.wsj.com/articles/many-company-hacks-go-undisclosed-to-sec-despite-regulator-efforts-11551218919.

Sayfayn, N., and S. Madnick. 2017. *Cybersafety analysis of the Maroochy Shire sewage spill, working paper cisl# 2017-09*. Cambridge, MA: Cybersecurity Interdisciplinary Systems Laboratory, Sloan School of Management, Massachusetts Institute of Technology.

Sobczak, B. 2019. "Hackers force water utilities to sink or swim." Accessed August 15, 2019. https://www.eenews.net/stories/1060131769.

SWAN Forum Interoperability Workgroup. 2016. "Communication in smart water networks." Accessed August 15, 2019. https://pdfs.semanticscholar.org/1aa7/59b64a0cf62364438f19648c57c64c5d4632.pdf.

Taormina, R., et al. 2018. "Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks." *J. Water Resour. Plann. Manage.* 144 (8): 04018048. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000969.

Taormina, R., and S. Galelli. 2018. "Deep-learning approach to the detection and localization of cyber-physical attacks on water distribution systems." *J. Water Resour. Plann. Manage.* 144 (10): 04018065. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000983.

Taormina, R., S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld. 2017. "Characterizing cyber-physical attacks on water distribution systems." *J. Water Resour. Plann. Manage.* 143 (5): 04017009. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000749.

USEPA. 2008. *Cyber security 101 for water utilities*. Washington, DC: USEPA.

USEPA. 2019a. *Information about public water systems*. Washington, DC: USEPA.

USEPA. 2019b. *Water sector cybersecurity brief for states*. Washington, DC: USEPA.

Vaas, L. 2017. "Beer + bitter former field engineer = hacked smart water meters." Accessed August 15, 2019. https://nakedsecurity.sophos.com/2017/06/28/beer-bitter-former-field-engineer-hacked-smart-water-meters.

Verizon. 2016. "Data breach digest. Scenarios from the field." Accessed August 15, 2019. https://enterprise.verizon.com/resources/reports/2016/data-breach-digest.pdf.

Verizon. 2017. "Data breach digest." Accessed August 15, 2019. https://enterprise.verizon.com/resources/reports/2017/data-breach-digest-2017-perspective-is-reality.pdf.

Walton, B. 2016. "Water sector prepares for cyberattacks." Accessed August 15, 2019. https://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks.

Walton, B. 2017. "Water utility cyberattack rings up hefty data charges." Accessed August 15, 2019. https://www.circleofblue.org/2017/water-management/water-utility-cyberattack-rings-hefty-data-charges.

WaterISAC (Water Information Sharing and Analysis Center). 2015. *10 basic cybersecurity measures: Best practices to reduce exploitable weaknesses and attacks*. Washington, DC: WaterISAC.

Weiss, J. 2010. *Protecting industrial control systems from electronic threats*. New York: Momentum Press.

White House. 2013. "Presidential policy directive—Critical infrastructure security and resilience." Accessed August 15, 2019. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

White House. 2017. "Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure." Accessed August 15, 2019. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure.

Willson, N. 2013. "Defensible security posture." Accessed August 15, 2019. https://nigesecurityguy.wordpress.com/2013/06/04/defensible-security-posture.

Zetter, K. 2011. "H(ackers)$_2$O: Attack on city water station destroys pump." Accessed August 15, 2019. https://www.wired.com/2011/11/hackers-destroy-water-pump.