



Delft University of Technology

A Review of Cybersecurity Incidents in the Water Sector

Hassanzadeh, Amin; Rasekh, Amin; Galelli, Stefano; Aghashahi, Mohsen; Taormina, Riccardo; Ostfeld, Avi; Banks, M. Katherine

DOI

[10.1061/\(ASCE\)EE.1943-7870.0001686](https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686)

Publication date

2020

Document Version

Accepted author manuscript

Published in

Journal of Environmental Engineering (United States)

Citation (APA)

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A Review of Cybersecurity Incidents in the Water Sector. *Journal of Environmental Engineering (United States)*, 146(5), 1-13. Article 03120003. [https://doi.org/10.1061/\(ASCE\)EE.1943-7870.0001686](https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686)

Important note

To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright

Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy

Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

A Review of Cybersecurity Incidents in the Water Sector

Amin Hassanzadeh, PhD¹, Amin Rasekh, PhD², Stefano Galelli, PhD³, Mohsen Aghashahi, MSc⁴, Riccardo Taormina, PhD⁵, Avi Ostfeld, PhD⁶, and M. Katherine Banks, PhD⁷

¹R&D Principal, Accenture Labs, Cyber Fusion Center, 800 North Glebe Road, Arlington, VA.

Email: amin.hassanzadeh@accenture.com

²Industry Advisor, Zachry Department of Civil Engineering, Texas A&M University, 400 Bizzell St, College Station, TX 77843.

³Assistant Professor, Pillar of Engineering Systems and Design, Singapore University of Technology and Design, 8 Somapah Rd., Singapore 487372, Singapore.

⁴Doctoral Student, Zachry Department of Civil Engineering, Texas A&M University, 400 Bizzell St, College Station, TX 77843.

⁵Assistant Professor, Department of Water Management, Faculty of Civil Engineering and Geosciences, Delft University of Technology, Stevinweg 1, 2628 CN Delft, the Netherlands.

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

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

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 have been selected and analyzed through a search strategy that included a variety of public information sources ranging from federal investigation

24 reports to scientific papers. For each individual incident, the situation, response, remediation, and
25 lessons learned are compiled and described. The findings of this review indicate an increase in the
26 frequency, diversity, and complexity of cyber-threats to the water sector. While the emergence of
27 new threats, such as ransomware or cryptojacking, is observed, a recurrence of similar vulnera-
28 bilities and threats, such as insider threats, is also evident, emphasizing the need for an adaptive,
29 cooperative, and comprehensive approach to water cyber-defense.

30 **INTRODUCTION**

31 The Water and Wastewater Sector (WWS) is considered by the U.S. Department of Homeland
32 Security (DHS) as one of the main targets for cyber-attacks amongst the sixteen lifeline infrastructure
33 sectors (White House 2013). Its safeguard against cybersecurity threats is considered a matter of
34 national priority (White House 2017). From 2012 to 2015, WWS received the highest number of
35 assessments from the Cybersecurity and Infrastructure Security Agency-Industrial Control Systems
36 (ICS-CERT 2016b), which routinely conducts on-site cybersecurity assessments for several critical
37 infrastructure sectors (ICS-CERT 2016b). The only exception was 2014, when the number of
38 assessments in the energy sector was slightly higher (ICS-CERT 2016b).

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

50 Recently, cybersecurity has piqued the interest and attention of the WWS industry and policy-

51 making entities. Several educational programs have been offered by the USEPA, DHS, the American
52 Water Works Association, and the Water Information Sharing & Analysis Center over the past few
53 years to raise awareness, train staff, and provide resources and tools to assist with cybersecurity
54 practices (WaterISAC 2015; ICS-CERT 2019; USEPA 2019b). This has been accompanied by
55 a rising interest in the research community (Amin et al. 2013; Rasekh et al. 2016; Ahmed et al.
56 2017; Formby et al. 2017; Taormina et al. 2017; Laszka et al. 2017; Taormina et al. 2018; Chandy
57 et al. 2018; Taormina and Galelli 2018; Housh and Ohar 2018; Ramotsoela et al. 2019). Within
58 this respect, there may exist valuable lessons and insights in the past cybersecurity incidents that
59 should be discovered and disseminated to inform the ongoing cyber-defense investments and efforts,
60 thereby enhancing their relevance and effectiveness. This requires a comprehensive compilation
61 and review of the these incidents; a public resource that is not currently available.

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

71 **INDUSTRIAL CONTROL NETWORKS**

72 In order to provide context for the analysis of the incidents, this section reviews traditional OT
73 networks, their integration with Information Technology (IT) networks, and standard architecture
74 designs proposed for ICS networks. We will refer to these architectures when reviewing some of the
75 incidents and map the attacker's activities to the architectural layers and targeted hardware/software.

76 ICS networks traditionally uses a system of hardware and software components—called Su-
77 pervisory Control and Data Acquisition (SCADA)—for process control, data collection, system

78 monitoring, communication with industrial devices, and log data storing. A typical SCADA sys-
79 tem architecture is depicted in Figure 1a: the lowest level generally consists of field elements (also
80 called end or dumb devices), such as sensors, pumps, and actuators. These elements are operated
81 by control devices, such as Programmable Logic Controllers (PLC) and Remote Terminal Units
82 (RTU). PLCs and RTUs are microcomputers that send control signals to the field elements, acquire
83 data, and transmit them to the central control station, such as a Master Terminal Unit (MTU). MTU
84 and RTUs/PLCs communicate and function in a master/slave model (through wired or wireless
85 networks, public telephone network, or even through the internet) to send commands, upload new
86 configurations, and monitor the field elements. Operators manage all these operations through
87 a Human Machine Interface (HMI) connected to the MTU that allows them to gather data, send
88 commands to remote sites, and change settings and configurations (Kruz 2005).

89 Figure 1b shows a typical water system architecture with RTUs and PLCs geographically-
90 dispersed in different sites. We have mapped different layers of a SCADA architecture to this
91 sample network, where field elements, such as valves or pressure gauges, are monitored by RTUs
92 with wireless antennas. The SCADA servers are located in a central control station (e.g., the
93 headquarters of a water utility) and remotely communicate with the RTUs and PLCS scattered in
94 the entire service area (SWAN Forum Interoperability Workgroup 2016).

95 For many years, SCADA systems, and, in general, OT networks in industrial environments, were
96 air-gapped—that is, not connected to corporate IT networks or internet. However, as technology
97 advanced, many organizations planned to consolidate overlapping IT and OT networks. This
98 approach aims at saving maintenance costs and integrating data collection and analysis (Kruz
99 2005). However, such integration comes at high security risks due to the following reasons:
100 1) OT networks have different operational priorities compared to IT networks—e.g., availability
101 vs. confidentiality—and one model may not fit both; 2) Most ICS devices and protocols are not
102 designed to support security features like data encryption or access control, and often support remote
103 access through radio modems; 3) Expensive legacy devices in ICS environments provide limited
104 visualization options to implement and evaluate security modifications; and, 4) Critical and real-

105 time business operations in OT, along with safety regulations, prevent immediate implementation
106 of remediation options that may require system interruptions. In light of the above, security experts
107 have proposed some work-around options to limit the access of users to the OT network. Other
108 efforts in the ICS security field are constantly improving standards, protocols, and devices to support
109 security features.

110 The new generation of converged IT-OT networks in industrial control systems, also referred to
111 as Industrial Internet of Things (IIoT), is no longer air-gapped. Figure 1c depicts a typical integrated
112 ICS network consisting of multiple levels and zones, also known as the Industrial Automation and
113 Control Systems (IACS) Security standard (ISA-62443) (Krutz 2005). A zone is in fact a set of
114 assets (IT or OT devices) grouped together to provide a subclass of services and applications for
115 the entire ICS network. The main zones can be described as follows:

- 116 • **Enterprise Zone** that includes assets for business logistics and enterprise systems, repre-
117 senting Level 4 and 5, respectively. This zone is also known as IT network.
- 118 • **Demilitarized Zone (DMZ)** that separates IT and OT networks, thus preventing direct
119 access to OT devices from the IT network. All corporate-accessible services (e.g., web,
120 email) reside in this zone.
- 121 • **Manufacturing Zone and Control Zone.** The former refers to the entire OT domain,
122 including Levels 0, 1, 2, and 3; the latter refers to Levels 0, 1, and 2, so it is equivalent to
123 the traditional ICS architecture shown in Figure 1a. Level 3 provides site-level operation
124 and asset management. Plant historian, production scheduling and reporting, patch and file
125 services reside at Level 3 (Hassanzadeh et al. 2015).

126 **ATTACK AND DEFENSE MODELS**

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

129 **Attack models**

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

139 In industrial environments, the attack life cycle is slightly different because of the different
140 architecture design shown in Figure 1c. The target in such networks can be an asset in one of the
141 three domains, namely, IT, DMZ, or OT. However, in most reported ICS incidents, the target is an
142 OT asset (Hassanzadeh et al. 2015), since the attacker gains access to the victim's environment
143 through the IT domain and then traverse to the OT infrastructure by launching multiple attacks.
144 This model is defined as the ICS Kill Chain, a multi-domain, multi-step approach that considers
145 ISA-62443 architectural levels and CKC steps together. Since the attacker may need to repeat
146 several CKC steps at each IT/OT level to laterally move within the network from one asset to
147 another (until he/she reaches the target), Hassanzadeh and Burkett (2018) proposed a spiral attack
148 model to accurately describe the attacker's activities within the converged IT/OT systems. Figure
149 2a shows a simplified version of this model, which is color-coded to map it to the IT/DMZ/OT
150 domains of Figure 1c. As depicted, an attacker may start with some reconnaissance activities in
151 outer layers of an organization that are more exposed to the public (e.g., web server, mail server),
152 and then find a vulnerable host that can be exploited. Once the first attack is delivered and executed,
153 the attacker is already inside the victim's network, and then escalates his/her privileges and move
154 laterally within the network towards the final target, which is placed in the lower levels. Note that
155 this is a generic model, so there might be attacks that do not necessarily start from Level 5—such

156 as an insider that uses OT workstations or a vulnerable server in the DMZ to launch an attack.

157 In light of the fact that an attacker operates in a chain of events (i.e., a set of single-step
158 intrusions), the diamond model of intrusion analysis proposes a formal method called “activity
159 thread” (Caltagirone et al. 2013). The method shows not only the attacker’s steps and causal
160 relation between them, but also a complete list of features for each of these steps. Figure 2b shows
161 the core and meta features of each single-step intrusion, or event. An activity thread in an industrial
162 environment is a directed graph (like the spiral set of arches in Figure 2a), where each vertex is an
163 event/intrusion (see Figure 2b) and links represent the relation between those intrusions from the
164 first step of the attack to the final target. As shown in Figure 2b, the four core features describe how
165 an *adversary* deploys a *capability* over some *infrastructure* against a *victim*. Let us further focus
166 on these features:

- 167 • **Adversary** is the actor or organization responsible for the attack. The adversary can be
168 categorized as insider or outsider and individual, group, or organization. This is usually
169 an unknown feature in most cyber-attacks. It is important to understand the distinction
170 between adversary operator (i.e., the actual hacker) and adversary customer (i.e., the entity
171 that benefits from the attack).
- 172 • **Capability** is the set of tools and techniques that are used by the attacker. The vulnerabilities
173 and configuration issues in the target environment define the capability of an attacker.
- 174 • **Infrastructure** is the physical and/or logical communication structure, such as email ad-
175 dresses or USB devices, used by the attacker to deliver the attack capabilities, maintain
176 control over them, and finally obtain results. The infrastructure can be owned or controlled
177 by the attacker or an intermediary (e.g., zombies hosts, botnets, or compromised email
178 accounts).
- 179 • **Victim** is the target that has vulnerabilities and configuration issues to provide attack
180 capabilities for the adversary. Victims are either persona (e.g., people or organizations) or
181 assets (e.g., networks, systems, accounts, or information).

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

194 **Defense models**

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

- 201 • **Basic Controls**, such as inventory and control of hardware/software assets, continuous
202 vulnerability management, or controlled use of administrative privileges;
- 203 • **Foundational Controls**, such as email and web browser protections, malware defenses, or
204 secure configuration for network devices like firewalls, routers, and switches;
- 205 • **Organizational Controls**, such as the implementation of a security awareness and training
206 program, incident response and management, penetration tests, and red team exercises.

207 Table 1 provides the complete list of CIS controls along with their corresponding category.

208 These controls are available and offered in different security tools and solutions. They can have
209 various impacts depending on their goal and implementation: 1) *detect* the attack; 2) *deny* or prevent
210 the attacker from accessing assets or information; 3) *disrupt* active malicious activities; 4) *degrade*
211 the impact of an attack; 5) *deceive* the attacker; or, 6) *contain* the malicious activity to a zone where
212 damages can be mitigated. Figure 3 shows how different security controls (tools and solutions)
213 can be used to protect an organization against an intrusion attempt at each CKC step (Hutchins
214 et al. 2011; Bodeau et al. 2013; Willson 2013). As an example, network-based intrusion detection
215 systems (NIDS), host-based intrusion detection systems (HIDS), or anti-virus (AV) solutions can
216 be used to detect exploitation activities. Similarly, trust zones can contain malicious activities
217 associated with multiple attack steps from delivery to action, and honeypots can deceive attackers
218 during several attack phases. AV solutions are mostly used to detect or disrupt attacks during the
219 delivery, exploitation, or installation phase, while data execution protection (DEP) techniques are
220 mostly used as a disruption mechanism.

221 In addition to traditional IT-based security controls, there exist several OT-specific security
222 controls—such as data-diode and unidirectional gateway, in-line command white listing, passive
223 asset discovery, passive OT intrusion detection (or anomaly detection), or patch and compliance
224 management—that are currently used in industrial networks. A closer look at these solutions
225 shows that they also fall under the categories mentioned above; however, they are designed to be
226 compatible with OT network protocols and standards. For example, unidirectional gateway ensures
227 a limited (if not zero) network interaction from the IT to the OT domain that should be considered
228 as a firewall with a very restricted communication rule consistent with the OT architecture and
229 its security needs. Hence, this OT-specific security control is a boundary defense control listed
230 in Table 1. Similarly, passive asset discovery in OT networks is a basic security control to create
231 an inventory of authorized and unauthorized devices (first control in Table 1). A technical report
232 published by the Department of Energy (Department of Energy 2005) lists 21 actions that can
233 increase the security of SCADA networks. Each action corresponds to one or multiple security
234 controls listed here.

INCIDENTS

In this review, a cybersecurity incident refers to an incident that has been maliciously launched from the cyber space to cause adverse consequences to a target entity. All available reports on disclosed, documented, and malicious cybersecurity incidents in WWS happened until the end of May 2019 were considered, but only the incidents with detailed and verified information were then selected. The information sources include 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 of this review did not conduct any direct investigation themselves. The review is not restricted to any particular geographic region. All incidents, here presented in chronological order, are true positives, with the exception of one incident. This was included due to the massive, negative cry-wolf effects it created in the aftermath of its disclosure. For each incident, we describe the situation, response/recovery (if available), and lessons learned.

1. Maroochy Water Services, Australia, 2000

Incident

Maroochy Shire is located about 100 kilometres 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 liters of sewage each day. During the period 1997–2000, Hunter Watertech Pty Ltd (HWT), a third-party contractor, installed PDS Compact 500 RTUs at all 142 sewage pumping stations. This enabled to remotely control and monitor 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, or altered configuration of the pumping stations. The incident resulted in the release of nearly one million liters of raw sewage into the river, local parks, and residential grounds. 500 meters 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 23rd, 2000, having

262 in his possession a Compact 500 computer, a two-way radio, a laptop, a transformer, and cables.
263 The suspect had served as a site supervisor for Hunter Watertech until resigning due to unspecified
264 disagreements (with effect from December 3rd, 1999). He was sentenced to two years in jail and
265 ordered to pay \$13,111 to the Council for the damage caused by the spill. The sewage spill and
266 its impacts were cleaned up. The process took days and required the deployment of substantial
267 resources.

268 The main hazard involved in this incident was the unauthorized access to the SCADA system,
269 which enabled the malevolent actor to release raw sewage into the surrounding environment. There
270 were no cybersecurity procedures, policies, or defenses present, and the service contract was
271 deficient or inadequate to handle the contractor's responsibilities. Considering that the attacker
272 was a former supervisor of the whole project, which controlled all pumping stations, the scale of
273 the impacts could have been more extensive. The attacker was indeed a skillful, insider adversary
274 with an intimate knowledge of the target system. The adoption of the NIST SP 800-53 control
275 protocols (Bodeau and Graubart 2013) would have arguably prevented all of the attacker's malicious
276 activities. A former employee's access to the network, for example, should indeed be terminated
277 immediately. (The sources used herein for this incident included District Court at Maroochydore
278 (2002), Abrams and Weiss (2008), and Sayfayn and Madnick (2017).)

279 **2. Pennsylvania Water Filtering Plant, U.S., 2006**

280 *Incident*

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

289 *Response and lessons learned*

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

298 **3. Tehama-Colusa Canal, U.S., 2007**

299 *Incident*

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

308 *Response and lessons learned*

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

314 This incident is another case of insider attack. In this case, however, the insider was reportedly
315 still an active employee of the affected entity at the time of the attack. (The sources used herein for

316 this incident included McMillan (2007), Weiss (2010), and RISI (2019).)

317 **4. Illinois Water Plant Pump Station, U.S., 2011 (a false alarm incident)**

318 *Incident*

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

325 *Response and lessons learned*

326 The FBI and DHS launched an investigation. DHS spokesman subsequently advised that “At
327 this time there is no credible corroborated data that indicates a risk to critical infrastructure entities
328 or a threat to public safety”. According to the DHS, the pump had malfunctioned multiple times
329 during the recent years. Additionally, the contractor with remote access to the computer system
330 was on a personal trip in Russia. Investigation of the log files and interviews with the personnel
331 collectively concluded that the reported attack was a false alarm.

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

338 **5. Key Largo Wastewater Treatment District, U.S., 2012**

339 *Incident*

340 In 2012, the former Chief Financial Officer (CFO) of Florida's Key Largo Wastewater Treatment
341 District illegally accessed the district's computer system to download emails and other personal

342 documents. He performed these actions using the credentials of other employees, after the district
343 did not renew his contract. He was arrested on account of felony charges, including computer
344 crime with intent to defraud, modify information without authority, and delete information from
345 the district's computer system.

346 *Response and lessons learned*

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

353 It is still not clear how the CFO got the credentials of his fellow employees. It is important for
354 employees to constantly update their passwords in order to reduce the risks associated with stolen
355 credentials. The CFO used these credentials to access the system from home, suggesting that no
356 second authentication factor was needed to access the computer systems. Similarly to the 'Kemuri
357 Water Company' incident (Incident 8 below), a two-factor authentication could have prevented this
358 attack. The attack was discovered thanks to routine checks, which should always been performed
359 extensively for systems containing sensitive and confidential data. (The sources used herein for this
360 incident included Government Technology (2012) and WPLG Inc (2012).)

361 **6. Bowman Avenue Dam, U.S., 2013**

362 *Incident*

363 The Bowman Avenue Dam is a small hydraulic infrastructure used to control floods in Blind
364 Brook creek (Rye, New York). A key component of the dam is a remotely-controllable sluice gate,
365 in operation since 2013, that controls the water flow as a function of water levels and temperatures
366 in the creek. Between August 28th and September 18th, 2013, hackers obtained "unauthorized
367 remote access" to the SCADA system; a cyber-attack that allowed them to gather information on
368 water levels, temperature, and the status of the sluice gate. The gate was manually disconnected

369 for maintenance at the time of the intrusion, so hackers could not have the opportunity of taking
370 direct control of the sluice gate. The attack was perpetrated with the aid of Google dorking, a
371 computer hacking technique that leverages Google search engine to locate specific strings—and
372 thereby vulnerabilities—in web applications, such as the one used to monitor and control the sluice
373 gate. The hacker’s action should not be classified as an intrusion, but rather as reconnaissance,
374 namely the first stage of the CKC (see Figure 2a), in which the attacker just gathers information on
375 a potential target by looking for publicly available information on the Internet. The attacker used a
376 standalone PC of the dam’s system to access its control network. However, at the time of attack,
377 the control system was only gathering water level information and storing it on a spreadsheet. “The
378 control system was attached to the Internet via a cellular modem but was directly Internet accessible
379 and not protected by a firewall or authentication access controls.”.

380 *Response and lessons learned*

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

390 **7. Five water utilities, U.S., 2014**

391 *Incident*

392 In the spring of 2014, five water utilities across three states in the U.S. experienced some
393 problems with their smart water meters. In particular, they faced inaccurate water bills and the
394 deactivation of the Tower Gateway Base Stations (TGB), which receive signals from the water
395 meters and transfer them to centralized facilities for monitoring and billing purposes. The first

396 incident was reported by Kennebec Water District (Maine), where the utility could not connect to
397 the TGB. Other nine attacks were reported in Spotswood (New Jersey), Egg Harbor (New Jersey),
398 Aliquippa (Pennsylvania), and New Kensington (Pennsylvania).

399 The attack was caused by a fired employee of the company that manufactured the smart water
400 meters—named company A in court’s documents—who gained unauthorized access to protected
401 computers. More specifically, the employee used to work as a field radio frequency engineer and
402 was fired in November 2013. A few weeks later, using his access to the base station network, he
403 conducted various malicious activities, such as changing the root passwords, modifying the TGB
404 radio frequency, and overwriting computer scripts.

405 *Response and lessons learned*

406 This abnormality drew the attention of the Federal government and caused investigations about
407 possible cyber-attacks against the water infrastructures. Since the attack disabled the communica-
408 tion between utilities and their data collection network, the organizations had to resume manual
409 data gathering. In addition, company A had to carry out forensic investigations at its own expenses
410 to identify the attacker, characterize the attacks, and find and repair the damage.

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

416 Even though the attacker was not a professional hacker, a default password allowed him to access
417 the TGB. This highlights the importance of implementing access control and revoking access rights
418 when someone is laid off. In addition, it is important to log and store in a safe place all logins and
419 user’s activities. If company A had kept track of log-ins earlier, investigators could have discovered
420 breaches dating prior to May 2014. This would have helped the investigations. (The sources used
421 herein for this incident included Department of Justice (2017), Cimpanu (2017), Vaas (2017), and
422 Gallagher (2017).)

8. Kemuri Water Company (a pseudonym), U.S., 2016

Incident

In 2016, an undisclosed water utility in the U.S. (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 mid-range computer system (AS400) 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 also conducted with the utility’s staff: they revealed that some staff members have been 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 actually proactive and not reactive.

A physical survey revealed the presence of a wired connection between the utility’s internet payment application and the AS400 system. Since the AS400 was open to the internet, it was concluded that access to the payment application would have also 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. In synthesis, 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.

450 Multiple exploitable vulnerabilities led to the breach, which could have led to more serious
451 consequences if the forensic investigation was not conducted earlier or the attackers had more
452 knowledge of the utility's OT and IT systems. Internet-facing servers and applications, such the
453 payment management application here, should not be connected to the SCADA. The utility had
454 relied on a single-factor authentication; this is not sufficient, and multi-factor authentication should
455 be used. Outdated systems, like the AS400 here, which formed a single point of failure, should not
456 be deployed, and installation of security patches should not be overlooked. Exfiltration of records
457 went unnoticed for a long time and in large amounts. There should be a monitoring mechanism in
458 place that oversees the transfer of data to enable early detection and response. (The sources used
459 herein for this incident included Verizon (2016) and Mahairas (2018).)

460 **9. An undisclosed utility, U.S., 2016**

461 *Incident*

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

466 *Response and lessons learned*

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

474 The situational awareness of the system administrator and prompt notification of ICS-CERT
475 proved to be effective in isolating and thwarting a potentially catastrophic intrusion. Under the
476 Critical Infrastructure Information Act of 2002 (CII Act), DHS has established the Protected Critical

477 Infrastructure Information (PCII) Program to assure the utilities that their submitted information
478 will not be disclosed. (The source used herein for this incident is ICS-CERT (2016a).)

479 **10. An undisclosed drinking water utility, U.S., 2016**

480 *Incident*

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

493 *Response and lessons learned*

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

497 **11. A regional water supplier, U.K., 2017**

498 *Incident*

499 A regional water supplier was notified by several of its clients that their online account details
500 were changed. After the clients credential were reset, it emerged that the details of some registered
501 bank accounts were also changed, so that refunds issued to the customers were transferred fraud-
502 ulently to these new bank accounts. In particular, the diverted refunds totaled over £500,000 and

503 were directed to two bank accounts in England. The banks holding these accounts were socially
504 engineered and allowed the holders to quickly transfer the majority of the funds to other bank
505 accounts in Dubai and the Bahamas. Subsequently, these funds were used to purchase Bitcoins,
506 which were then transferred to addresses associated with a Bitcoin mixing service, thus preventing
507 any subject to be identified by following this trail further.

508 *Response and lessons learned*

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

527 This insider attack examined here suggests that management should also ensure that partners
528 having access to critical data perform stringent background checks on their employees. (The source
529 used herein for this incident is Verizon (2017).)

530 **12. A European water utility, 2018**

531 *Incident*

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

541 *Response and lessons learned*

542 The security firm informed the water utility about the crypto-mining malware and infected
543 servers. The recovery scheme included updating the anti-virus software on some servers as well
544 as tightening the firewall security. The updated anti-virus software was successful in detecting the
545 CoinMiner malware.

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

552 **13. Onslow Water and Sewer Authority, U.S., 2018**

553 *Incident*

554 Onslow Water and Sewer Authority, a water utility company in Jacksonville (North Carolina)
555 was targeted by cyber-criminals in October of 2018. Timed right in the wake of Hurricane Florence,
556 the attack soon escalated into a sophisticated ransomware attack that locked out employees and

557 encrypted databases, leaving the utility with limited computing capabilities. The hack began with
558 persistent cyber-attacks through a virus known as EMOTET. With the EMOTET virus infection
559 persisting, the authority reached out to outside security experts to investigate and respond to the at-
560 tack. At approximately 3 am on Saturday October 13th, while the investigations were still underway,
561 the malware launched a more sophisticated virus known as RYUK. The IT team immediately dis-
562 connected the authority’s facilities from the internet. Nevertheless, the situation soon exacerbated
563 and the virus encrypted files and data. The authority suspects that the attack has been a targeted
564 one because the hackers chose a target that was recently hit by a natural disaster. Moreover, the
565 sophisticated virus was launched at 3 am on a Saturday—a time in which the authority was most
566 vulnerable. The authority soon received one email from the cyber criminals demanding payment
567 to decrypt the damaged files and data. The authority dismissed the offer and stated it will not
568 “negotiate with criminals nor bow to their demands.”

569 *Response and lessons learned*

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

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

579 **14. Fort Collins Loveland Water District, U.S., 2019**

580 *Incident*

581 Fort Collins Loveland Water District serves customers in parts of Fort Collins, Loveland,
582 Timnath, Windsor, and Larimer County (Colorado). On February 11th, 2019, the staff of the Fort
583 Collins Loveland Water District and South Fort Collins Sanitation District were unable to access

584 technical data. Daily operations and customers' data were not believed to have been compromised.
585 The utility had fallen victim to a ransomware cyber-attack. The hackers demanded a ransom to
586 restore access (the amount of ransom payment demanded has not been disclosed to the public).
587 The district declined to pay the ransom.

588 *Response and lessons learned*

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

593 This is another case of ransomware attack in which the victim declined to pay a ransom. Data
594 segmentation and segregation proven to be a helpful practice in safeguarding sensitive customer
595 and daily operation data. Hiring a third-party vendor to handle customer payments prevented the
596 customer data to be compromised. The practice of hiring third-party vendors, however, creates
597 its own risks, as it was also manifested by Incident 11. (The sources used herein for this incident
598 included Ferrier (2019) and Sobczak (2019).)

599 **15. Riviera Beach Water Utility, U.S., 2019**

600 *Incident*

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

607 *Response and lessons learned*

608 A few days after the attack, the city council unanimously voted to authorize its insurer to pay
609 65 bitcoins, approximately \$600,000, to the attackers. The city would pay an additional \$25,000 as

610 insurance deductibles out of its budget. Two weeks after the attack was disclosed, the IT department
611 could bring the city’s website and email services fully operational, while the water pump stations
612 and water quality testing systems were only partially available. Although water quality sampling
613 had to be performed manually, the city council’s spokeswoman assured that water quality itself was
614 never in jeopardy. The FBI, Secret Service, and DHS investigated the attack and recommended the
615 city not to pay the ransom. Regardless of paying the ransom, as of June 20th, 2019, the sensitive
616 data being encrypted by hackers were still inaccessible.

617 While waiting for the attackers to share a decryption key, the local government authorized
618 spending more than \$900,000 to buy new computer hardware—purchases which were planned for
619 next year. According to a councilperson, most of the existing hardware was old and outdated, which
620 made it vulnerable to the cyber-attack. In addition, the city’s computer network was not updated,
621 and patches were not installed on time.

622 It is known that local governments and small public utilities are less prepared for cyber-attacks,
623 since they lack the budget and professionals needed to secure their IT and OT systems. That
624 said, basic cybersecurity training raises awareness, and reduces the possibility of succumbing to
625 devastating attacks unleashed by the naivety of uninformed employees, such as the case for Riviera
626 Beach. Although paying a ransom looks like the easiest way to solve the problem, FBI and security
627 experts suggest never to pay ransom as it only encourages future criminal activity. Preventing
628 cyber-attacks from happening is always the best practice. (The sources used herein for this incident
629 included Doris (2019), Mazzei (2019), and O’Donnell (2019).)

630 **DISCUSSION**

631 As outlined in the previous section, the complexity of cyber-incidents in WWS has increased
632 during the last two decades. In some earlier incidents, such as the 2000 Maroochy Water Services
633 hack, an insider simply and directly gained access to the OT controllers and performed malicious
634 activities, while in some recent attacks, such the 2016 Kemuri Water Company hack, several IT
635 and OT workstations were compromised by outsiders using multi-step attack techniques. In this
636 section, we review and analyze some key points of the aforementioned incidents from both attacker

637 and defender's perspectives.

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

655 Attackers are usually grouped based on their capabilities, motivations, and goals. Based on these
656 characteristics, various groups of attackers are defined such as script kiddies (curious, unskilled
657 individual), cyberterrorists (physical damage goals), cybercriminals (financial goals), hacktivists
658 (social or political goals), and state-sponsored actors. It is worth mentioning that some other
659 groups, such as cyber researchers, white/black hats and internal actors, have been also proposed in
660 the literature (Ablon 2018). Regardless of their goals and capabilities, attackers can be insider or
661 outsider. Table 3 summarizes the type of attackers, their target assets and domains, and their final
662 action on the observed target. Attacker and group for Incident 4 are not available simply because the
663 incident was later confirmed to be a false alarm. It is observed that insiders are common adversaries

664 in the water sector, as reported for the Key Largo Wastewater Treatment District, Maroochy Shire,
665 Tehama Colusa Canal Authority, the five Eastern water utilities attacks, and a regional water
666 supplier hack (Incidents 1, 3, 5, 7, and 11). This suggests that management and security teams
667 should be more cognizant of changes in the behaviors of employees. For example, in the Maroochy
668 Water attack, the attacker was no longer an employee. However, he still had access to the wireless
669 network. Thus, he can be considered as an insider causing physical and financial damages (both
670 cyber-criminal and cyber-terrorist) who changed the configuration of several OT controllers. In
671 some similar examples, such as Incidents 3, 5, and 7, former employees or contractors tried to cause
672 harm (financially or physically) through an unauthorized access to the IT or OT systems. In case
673 of Incident 7, the attacker chose multiple targets in different domains of five utilities.

674 The attacker in the second incident was most likely a script kiddie (SK) outsider, who installed
675 malware on the victim's computer to gain access to the internal information and distribute emails
676 and information—there is no evidence of other groups of attackers in the public report. However,
677 it is known that Attack 8 is performed by state-sponsored parties who targeted multiple IT and OT
678 systems that resulted in the data exfiltration and manipulation of chemicals and flow rates. Incident
679 4 is known as a false alarm; however, several operational issues were observed at the same time,
680 thereby confusing the investigation team. As shown in Table 3, recent incidents (since 2017) appear
681 to have a more complex nature. The attackers, insider or outsider, have been targeting databases,
682 files, and account servers of the victims for financial purposes. As organizations advance and
683 integrate their IT and OT systems and limit the OT systems from accessing to internet directly, the
684 IT systems become of more interest for attackers and the entry point to the victim's network. The
685 most interesting and unusual attack in this study is perhaps Incident 12, where attackers deployed a
686 cryptocurrency mining code on the OT network of the target utility (most likely downloaded from
687 malicious websites) to use the computational resources of OT machines as part of a mining pool
688 that creates or discovers digital currency.

689 There is no single defense mechanism that can protect WWS against cyber threats, so the
690 defense teams should use any mechanism (e.g., detect, deny, deceive) offered by critical security

691 controls (CSC) (CIS 2019) (see Table 1). In Table 4, we outline the most needed protection
692 mechanisms and top-three basic and foundational CSC for the attacks described in this study. The
693 foundational CSC are associated to specific architectural levels, based on the attacker’s first step
694 and weakest point of the victim’s network. We note that in almost all incidents there exists a
695 lack of organizational controls, such as “Security Skills Assessment and Appropriate Training to
696 Fill Gaps” or “Incident Response and Management.” Although many organizations use proactive
697 approaches—such as routine vulnerability and threat assessment or adversary simulation (red
698 teaming - CSC 20)—to find security flaws in their network, most of the reviewed incidents were
699 not detected proactively. Reactive security strategy, as seen in most industrial networks triggers,
700 is “respond when it happens.” Table 4 also shows that most of WWS networks suffer from a lack
701 of preventive security mechanisms (column Deny in Figure 3), that is, the first line of defense in
702 cybersecurity practice.

703 **EPILOGUE**

704 Water systems across the globe have increasingly become potential targets for cyber-criminals.
705 This study presented a review of fifteen cybersecurity incidents in the water and wastewater sector
706 within a context of industrial network architectures and attack-defense models. The incidents
707 cover a wide variety of vulnerabilities and situations. The incidents span over 18 years, from the
708 Maroochy Shire Sewage Treatment Plant insider attack in 2001 to the Riviera Beach Water Utility
709 ransomware attack in 2019. This review is an informative resource to guide securing of industrial
710 control systems in WWS and other lifeline sectors against cyber-threats. The sheer diversity of the
711 systems, attackers, and consequences associated with the incidents dictate a need for inclusive and
712 comprehensive vulnerability assessments, as well as risk mitigation, preparedness, response, and
713 recovery studies that account for such extreme heterogeneity.

714 Since the reports by official agencies denote a large number of cybersecurity incidents in the
715 WWS, this review may not be inclusive of all incidents. Many of them may not indeed be made
716 public. The framework developed by this study, however, was structured and designed such that it
717 can readily accommodate extensions and updates as more incidents are possibly disclosed (or take

718 place in the future). The development and maintenance of an online version of this repository is
719 believed to be a significant future endeavor to pursue.

720 **DATA AVAILABILITY**

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

722 **ACKNOWLEDGMENTS**

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

728 **REFERENCES**

- 729 Ablon, L. (2018). *Data Thieves: The Motivations of Cyber Threat*
730 *Actors and Their Use and Monetization of Stolen Data*. RAND
731 https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf.
732 (Aug. 15, 2019).
- 733 Abrams, M. and Weiss, J. (2008). “Malicious control system cyber security attack case study—
734 maroochy water services, australia.” *McLean, VA: The MITRE Corporation*.
- 735 Ahmed, C. M., Murguia, C., and Ruths, J. (2017). “Model-based attack detection scheme for smart
736 water distribution networks.” *Proceedings of the 2017 ACM on Asia Conference on Computer*
737 *and Communications Security*, ACM, 101–113.
- 738 Amin, S., Litrico, X., Sastry, S., and Bayen, A. M. (2013). “Cyber security of water scada
739 systems—part i: Analysis and experimentation of stealthy deception attacks.” *IEEE Transactions*
740 *on Control Systems Technology*, 21(5), 1963–1970.
- 741 Bodeau, D. and Graubart, R. (2013). “Cyber resiliency and nist special publication 800-53 rev. 4
742 controls.” *MITRE, Tech. Rep*.

743 Bodeau, D., Graubart, R., and Heinbockel, W. (2013). “Characterizing effects on the cyber adver-
744 sary.” *MTR130432, MITRE Corporation, November.*

745 Caltagirone, S., Pendergast, A., and Betz, C. (2013). *Data Thieves: The Motivations of Cyber*
746 *Threat Actors and Their Use and Monetization of Stolen Data.* Center For Cyber Intelligence
747 Analysis and Threat Research Hanover Md.

748 Cava, M. D. (2018). *Uber to pay \$148 million over undisclosed data breach that ex-CEO paid hack-*
749 *ers to keep quiet.* USA Today . [https://www.usatoday.com/story/tech/news/2018/09/26/uber-pay-](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)
750 [148-million-over-undisclosed-data-breach-ex-ceo-paid-hackers-keep-quiet/1432335002.](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) (Aug.
751 15, 2019).

752 Chandy, S. E., Rasekh, A., Barker, Z. A., and Shafiee, M. E. (2018). “Cyberattack detection using
753 deep generative models with variational inference.” *Journal of Water Resources Planning and*
754 *Management*, 145(2), 04018093.

755 Cimpanu, C. (2017). *Fired Employee Hacks and Shuts Down Smart Water Readers in Five US Cities.*
756 *Bleeping Computer LLC* . [https://www.bleepingcomputer.com/news/security/fired-employee-](https://www.bleepingcomputer.com/news/security/fired-employee-hacks-and-shuts-down-smart-water-readers-in-five-us-cities)
757 [hacks-and-shuts-down-smart-water-readers-in-five-us-cities.](https://www.bleepingcomputer.com/news/security/fired-employee-hacks-and-shuts-down-smart-water-readers-in-five-us-cities) (Aug. 15, 2019).

758 CIS (2019). *CIS Controls.* Center for Internet Security, Inc. [https://www.cisecurity.org/controls.](https://www.cisecurity.org/controls)
759 (Aug. 15, 2019).

760 Cuomo, A. (2016). *Statement from Governor Andrew M. Cuomo on Cyber Attack Charges*
761 *Announced By U.S. Attorney General Loretta Lynch and FBI Director James Comey In-*
762 *volving the Bowman Avenue Dam in Westchester County.* The Government of New York
763 State . [https://www.governor.ny.gov/news/statement-governor-andrew-m-cuomo-cyber-attack-](https://www.governor.ny.gov/news/statement-governor-andrew-m-cuomo-cyber-attack-charges-announced-us-attorney-general-loretta)
764 [charges-announced-us-attorney-general-loretta.](https://www.governor.ny.gov/news/statement-governor-andrew-m-cuomo-cyber-attack-charges-announced-us-attorney-general-loretta) (Aug. 15, 2019).

765 Department of Energy (2005). *21 Steps to Improve Cyber Security of SCADA Network.* Department
766 of Energy . [https://www.hsdl.org/?abstract&did=1826.](https://www.hsdl.org/?abstract&did=1826) (Aug. 15, 2019).

767 Department of Justice (2017). *Bala Cynwyd Man Sentenced to Prison for Hacking Computers*
768 *of Public Utilities* . [https://www.justice.gov/usao-edpa/pr/bala-cynwyd-man-sentenced-prison-](https://www.justice.gov/usao-edpa/pr/bala-cynwyd-man-sentenced-prison-hacking-computers-public-utilities)
769 [hacking-computers-public-utilities.](https://www.justice.gov/usao-edpa/pr/bala-cynwyd-man-sentenced-prison-hacking-computers-public-utilities) (Aug. 15, 2019).

770 District Court at Maroochydore (2002). *Appeal against Conviction and Sentence Proceedings*
771 *regarding Appellant Vitek Boden*. Supreme Court of Queensland, Queensland, Australia .
772 <https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf>. (Aug. 15, 2019).

773 Doris, T. (2019). *Why Riviera Beach agreed to pay a \$600,000 ransom pay-*
774 *ment to regain data access... and will it work?* The Palm Beach Post.
775 [https://www.palmbeachpost.com/news/20190619/why-riviera-beach-agreed-to-pay-600000-](https://www.palmbeachpost.com/news/20190619/why-riviera-beach-agreed-to-pay-600000-ransom-payment-to-regain-data-access-and-will-it-work)
776 [ransom-payment-to-regain-data-access-and-will-it-work](https://www.palmbeachpost.com/news/20190619/why-riviera-beach-agreed-to-pay-600000-ransom-payment-to-regain-data-access-and-will-it-work). (Aug. 15, 2019).

777 Ferrier, P. (2019). *Cyberattacker demands ransom from Northern Colorado util-*
778 *ity*. The Coloradoan. [https://www.coloradoan.com/story/money/2019/03/14/cyberattacker-](https://www.coloradoan.com/story/money/2019/03/14/cyberattacker-demands-ransom-colorado-utility/3148951002)
779 [demands-ransom-colorado-utility/3148951002](https://www.coloradoan.com/story/money/2019/03/14/cyberattacker-demands-ransom-colorado-utility/3148951002). (Aug. 15, 2019).

780 Formby, D., Durbha, S., and Beyah, R. (2017). “Out of control: Ransomware for industrial control
781 systems.” *RSA Conference*.

782 Gallagher, S. (2017). *Some beers, anger at former employer, and root access add up to a year*
783 *in prison*. Arstechnica . [https://arstechnica.com/information-technology/2017/06/ex-technician-](https://arstechnica.com/information-technology/2017/06/ex-technician-convicted-of-possibly-drunken-attack-on-smart-water-meter-system)
784 [convicted-of-possibly-drunken-attack-on-smart-water-meter-system](https://arstechnica.com/information-technology/2017/06/ex-technician-convicted-of-possibly-drunken-attack-on-smart-water-meter-system). (Aug. 15, 2019).

785 Government Technology (2012). *Report: Hacking Lands Florida Wastewater Official in Hot*
786 *Water*. Government Technology. [https://www.govtech.com/public-safety/Report-Hacking-Lands-](https://www.govtech.com/public-safety/Report-Hacking-Lands-Florida-Wastewater-Official-in-Hot-Water.html)
787 [Florida-Wastewater-Official-in-Hot-Water.html](https://www.govtech.com/public-safety/Report-Hacking-Lands-Florida-Wastewater-Official-in-Hot-Water.html). (Aug. 15, 2019).

788 Hassanzadeh, A. and Burkett, R. (2018). “SAMIIT: Spiral attack model in iiot mapping security
789 alerts to attack life cycle phases.” *2018 International Symposium for ICS and SCADA Cyber*
790 *Security Research (ICS-CSR 2018)*, eWiC, 11–20.

791 Hassanzadeh, A., Modi, S., and Mulchandani, S. (2015). “Towards effective security control
792 assignment in the industrial internet of things.” *2015 IEEE 2nd World Forum on Internet of*
793 *Things (WF-IoT)*, IEEE, 795–800.

794 Housh, M. and Ohar, Z. (2018). “Model-based approach for cyber-physical attack detection in water
795 distribution systems.” *Water research*, 139, 132–143.

796 Hutchins, E. M., Cloppert, M. J., and Amin, R. M. (2011). “Intelligence-driven computer network

797 defense informed by analysis of adversary campaigns and intrusion kill chains.” *Leading Issues*
798 *in Information Warfare & Security Research*, 1(1), 80.

799 ICS-CERT (2016a). *ICS-CERT Monitor – March/April 2016*. U.S. Department of Homeland Se-
800 curity, Washington, DC.

801 ICS-CERT (2016b). *NCCIC/ICS-CERT year in review: FY 2015*. U.S. Department of Homeland
802 Security, Washington, DC.

803 ICS-CERT (2019). *DHS Critical Infrastructure Cyber Community Voluntary Program*. Department
804 of Homeland Security. <https://www.us-cert.gov/ccubedvp>. (Aug. 15, 2019).

805 Jerome, S. (2017). *Utility Cyberattack Targets Bandwidth, Not Water*. Water Online.
806 <https://www.wateronline.com/doc/utility-cyberattack-targets-bandwidth-not-water-0001>. (Aug.
807 15, 2019).

808 Kerner, S. (2018). *Water Utility in Europe Hit by Cryptocurrency Malware Mining At-*
809 *tack*. eWeek. [https://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-](https://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack)
810 [malware-mining-attack](https://www.eweek.com/security/water-utility-in-europe-hit-by-cryptocurrency-malware-mining-attack). (Aug. 15, 2019).

811 Krutz, R. L. (2005). *Securing SCADA systems*. John Wiley & Sons.

812 Kutner, M. (2016). *Alleged Dam Hacking Raises Fears of Cyber Threats to Infrastructure*.
813 Newsweek. <https://www.newsweek.com/cyber-attack-rye-dam-iran-441940>. (Aug. 15, 2019).

814 Lach, E. (2016). *Cyber War Comes to the Suburbs*. The New Yorker.
815 <https://www.newyorker.com/tech/annals-of-technology/cyber-war-comes-to-the-suburbs>.
816 (Aug. 15, 2019).

817 Laszka, A., Abbas, W., Vorobeychik, Y., and Koutsoukos, X. (2017). “Synergic security for smart
818 water networks: Redundancy, diversity, and hardening.” *Proceedings of the 3rd International*
819 *Workshop on Cyber-Physical Systems for Smart Water Networks*, ACM, 21–24.

820 Mahairas, Ari; Beshar, P. (2018). *A Perfect Target for Cybercriminals*. The New York Times.
821 <https://www.nytimes.com/2018/11/19/opinion/water-security-vulnerability-hacking.html>.
822 (Aug. 15, 2019).

823 Martin, A. (2018). *Russian hackers targeted Ukraine’s water supply, security service claims*.

824 Sky News. [https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-](https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826)
825 [service-claims-11432826](https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826). (Aug. 15, 2019).

826 Mazzei, P. (2019). *Hit by Ransomware Attack, Florida City Agrees to Pay Hackers \$600,000*.
827 The New York Times. [https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-](https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html)
828 [ransom.html](https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html). (Aug. 15, 2019).

829 McGurk, S. P. (2008). "Industrial control systems security: Protecting the critical infrastructure."
830 *U.S. Department of Homeland Security*.

831 McMillan, R. (2006). *Hackers break into water system network*. ComputerWorld.
832 [https://www.computerworld.com/article/2547938/hackers-break-into-water-system-](https://www.computerworld.com/article/2547938/hackers-break-into-water-system-network.html)
833 [network.html](https://www.computerworld.com/article/2547938/hackers-break-into-water-system-network.html). (Aug. 15, 2019).

834 McMillan, R. (2007). *Insider charged with hacking California canal system*. Com-
835 *puterWorld*. [https://www.computerworld.com/article/2540235/insider-charged-with-hacking-](https://www.computerworld.com/article/2540235/insider-charged-with-hacking-california-canal-system.html)
836 [california-canal-system.html](https://www.computerworld.com/article/2540235/insider-charged-with-hacking-california-canal-system.html). (Aug. 15, 2019).

837 Nakashima, E. (2011). *Water-pump failure in Illinois wasn't a cyberattack after all*. Wash-
838 *ington Post*. [https://www.washingtonpost.com/world/national-security/water-pump-failure-in-](https://www.washingtonpost.com/world/national-security/water-pump-failure-in-illinois-wasnt-cyberattack-after-all/2011/11/25/gIQACgTewNstory.html)
839 [illinois-wasnt-cyberattack-after-all/2011/11/25/gIQACgTewNstory.html](https://www.washingtonpost.com/world/national-security/water-pump-failure-in-illinois-wasnt-cyberattack-after-all/2011/11/25/gIQACgTewNstory.html). (Aug. 15, 2019).

840 Newman, L. (2018). *Now Cryptojacking Threatens Critical Infrastructure, Too*. Wired.
841 <https://www.wired.com/story/cryptojacking-critical-infrastructure>. (Aug. 15, 2019).

842 NIST (2012). *Computer Security Incident Handling Guide*. National Institute of Standards and
843 *Technology*, Washington, DC.

844 O'Donnell, L. (2019). *Post-Ransomware Attack, Florida City Pays \$600K*. Threatpost.
845 <https://threatpost.com/ransomware-florida-city-pays-600k-ransom/145869>. (Aug. 15, 2019).

846 ONWASA (2018). *Cyber-criminals target critical utility in hurricane-*
847 *ravaged area*. Onslow Water and Sewer Authority, Jacksonville, NC
848 [https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-](https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A)
849 [A](https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A). (Aug. 15, 2019).

850 Parish, J. (2011). *Illinois water plant 'hack' was denied by FBI and DHS and later proved*

851 *a false alarm*. The Verge. [https://www.theverge.com/2011/12/1/2604353/illinois-water-plant-](https://www.theverge.com/2011/12/1/2604353/illinois-water-plant-hack-was-denied-by-fbi-and-dhs-and-later-proved)
852 [hack-was-denied-by-fbi-and-dhs-and-later-proved](https://www.theverge.com/2011/12/1/2604353/illinois-water-plant-hack-was-denied-by-fbi-and-dhs-and-later-proved). (Aug. 15, 2019).

853 Radiflow (2018). *Detection of a Crypto-Mining Malware Attack at a Water Utility*. Radiflow,
854 Mahwah, NJ. [https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-](https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility)
855 [at-a-water-utility](https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility). (Aug. 15, 2019).

856 Ramotsoela, D. T., Hancke, G. P., and Abu-Mahfouz, A. M. (2019). “Attack detection in water dis-
857 tribution systems using machine learning.” *Human-centric Computing and Information Sciences*,
858 9(1), 13.

859 Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., and Banks, M. K. (2016). “Smart water
860 networks and cyber security.” *Journal of Water Resources Planning and Management*, 142(7).

861 RISI (2019). *The Repository of Industrial Security Incidents*. RISI Online Incident Database.
862 <https://www.risidata.com>. (Aug. 15, 2019).

863 Rubin, G. T. (2019). *Many Company Hacks Go Undisclosed to SEC Despite Regulator Efforts*.
864 The Wall Street Journal. [https://www.wsj.com/articles/many-company-hacks-go-undisclosed-](https://www.wsj.com/articles/many-company-hacks-go-undisclosed-to-sec-despite-regulator-efforts-11551218919)
865 [to-sec-despite-regulator-efforts-11551218919](https://www.wsj.com/articles/many-company-hacks-go-undisclosed-to-sec-despite-regulator-efforts-11551218919). (Aug. 15, 2019).

866 Sayfayn, N. and Madnick, S. (2017). “Cybersafety analysis of the maroochy shire sewage spill,
867 working paper cisl# 2017-09.” *Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan*
868 *School of Management, Massachusetts Institute of Technology*, 2017–09.

869 Sobczak, B. (2019). *Hackers force water utilities to sink or swim*. E&E News.
870 <https://www.eenews.net/stories/1060131769>. (Aug. 15, 2019).

871 SWAN Forum Interoperability Workgroup (2016). *Communication in*
872 *Smart Water Networks*. SWAN Forum, Surrey, United Kingdom.
873 <https://pdfs.semanticscholar.org/1aa7/59b64a0cf62364438f19648c57c64c5d4632.pdf>. (Aug.
874 15, 2019).

875 Taormina, R. and Galelli, S. (2018). “Deep-learning approach to the detection and localization of
876 cyber-physical attacks on water distribution systems.” *Journal of Water Resources Planning and*
877 *Management*, 144(10), 04018065.

878 Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., and Ostfeld, A. (2017). “Characterizing
879 cyber-physical attacks on water distribution systems.” *Journal of Water Resources Planning and*
880 *Management*, 143(5), 04017009.

881 Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., Ostfeld, A., Eliades, D. G., Aghashahi,
882 M., Sundararajan, R., Pourahmadi, M., Banks, M. K., et al. (2018). “Battle of the attack detection
883 algorithms: Disclosing cyber attacks on water distribution networks.” *Journal of Water Resources*
884 *Planning and Management*, 144(8), 04018048.

885 USEPA (2008). *Cyber Security 101 for Water Utilities*. U.S. Environmental Protection Agency,
886 Washington, DC.

887 USEPA (2019a). *Information about Public Water Systems*. U.S. Environmental Protection Agency.

888 USEPA (2019b). *Water Sector Cybersecurity Brief for States*. Washington, DC.

889 Vaas, L. (2017). *Beer + bitter former field engineer = hacked smart water meters*. Naked Security
890 . [https://nakedsecurity.sophos.com/2017/06/28/beer-bitter-former-field-engineer-hacked-smart-](https://nakedsecurity.sophos.com/2017/06/28/beer-bitter-former-field-engineer-hacked-smart-water-meters)
891 [water-meters](https://nakedsecurity.sophos.com/2017/06/28/beer-bitter-former-field-engineer-hacked-smart-water-meters). (Aug. 15, 2019).

892 Verizon (2016). *Data Breach Digest-Scenarios from the field*. Verizon .
893 <https://enterprise.verizon.com/resources/reports/2016/data-breach-digest.pdf>. (Aug. 15,
894 2019).

895 Verizon (2017). *Data Breach Digest*. Verizon . [https://enterprise.verizon.com/resources/reports/2017/data-](https://enterprise.verizon.com/resources/reports/2017/data-breach-digest-2017-perspective-is-reality.pdf)
896 [breach-digest-2017-perspective-is-reality.pdf](https://enterprise.verizon.com/resources/reports/2017/data-breach-digest-2017-perspective-is-reality.pdf). (Aug. 15, 2019).

897 Walton, B. (2016). *Water Sector Prepares For Cyberattacks*. Circle of Blue .
898 <https://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks>. (Aug. 15, 2019).

899 Walton, B. (2017). *Water Utility Cyberattack Rings Up Hefty Data Charges*. Circle
900 of Blue [https://www.circleofblue.org/2017/water-management/water-utility-cyberattack-rings-](https://www.circleofblue.org/2017/water-management/water-utility-cyberattack-rings-hefty-data-charges)
901 [hefty-data-charges](https://www.circleofblue.org/2017/water-management/water-utility-cyberattack-rings-hefty-data-charges). (Aug. 15, 2019).

902 WaterISAC (2015). *10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weak-*
903 *nesses and Attacks*. The Water Information Sharing and Analysis Center, Washington, DC.

904 Weiss, J. (2010). *Protecting industrial control systems from electronic threats*. Momentum Press.

905 White House (2013). *Presidential Policy Directive–Critical Infrastructure Security and*
906 *Resilience. PPD-21*. Washington, DC. [https://obamawhitehouse.archives.gov/the-press-](https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)
907 [office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil](https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil). (Aug.
908 15, 2019).

909 White House (2017). *Presidential Executive Order on Strengthening the Cy-*
910 *bersecurity of Federal Networks and Critical Infrastructure*. Washington, DC.
911 [https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-](https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure)
912 [cybersecurity-federal-networks-critical-infrastructure](https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure). (Aug. 15, 2019).

913 Willson, N. (2013). *Defensible Security Posture*. Nige the Security Guy
914 <https://nigesecurityguy.wordpress.com/2013/06/04/defensible-security-posture>. (Aug. 15,
915 2019).

916 WPLG Inc (2012). *Keys man charged in computer hacking*. WPLG Inc
917 <https://www.local10.com/news/florida/keys-man-charged-in-computer-hacking>. (Aug. 15,
918 2019).

919 Zetter, K. (2011). *H(ackers)2o: attack on city water station destroys pump*. Wired.
920 <https://www.wired.com/2011/11/hackers-destroy-water-pump>. (Aug. 15, 2019).

921
922
923
924
925

List of Tables

1 List of CIS Controls (CIS 2019). 37

2 Summary of the incidents. 38

3 Adversary Analysis. 39

4 Defense Analysis. 40

TABLE 1. List of CIS Controls (CIS 2019).

#	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 backup 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 & 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

TABLE 2. Summary of the incidents.

#	Location	Year	Target System	Investigator	Primary Impact
1	Australia	2000	Wastewater	HWT & Queensland EPA	Environmental pollution
2	PA, U.S.	2006	Water treatment	FBI	Data breach
3	CA, U.S.	2007	Irrigation	System personnel	Water theft
4	IL, U.S.	2011	Water plant	DHS	Cry-wolf effects
5	FL, U.S.	2012	Wastewater	System personnel	Data breach
6	NY, U.S.	2013	Dam	Justice Department	Data breach
7	U.S.	2013	Water utility	Third-party provider	Data manipulation
8	U.S.	2016	Water utility	Verizon Security	Control manipulation
9	U.S.	2016	Water utility	DHS	Data breach
10	U.S.	2016	Water utility	DHS	Bandwidth theft
11	U.K.	2017	Water supplier	Verizon Security	Financial impact
12	Europe	2018	Water utility	Radiflow	Resource theft
13	NC, U.S.	2018	Water utility	State and Federal	Data loss
14	CO, U.S.	2019	Water district	System personnel	Denial of access
15	FL, U.S.	2019	Water utility	FBI, DHS and Secret Services	Data loss

TABLE 3. Adversary Analysis.

#	Attacker	Group	Target	Domain	Action
1	Insider	C&T	RTU/PLC	OT	Configuration Change
2	Outsider	SK	Workstations	IT	Data Exfiltration
3	Insider	C&T	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 DB	IT	Unauthorized access
12	Outsider	Cybercriminal	SCADA/HMI	OT	Cryptojacking
13	Outsider	Cybercriminal	Info. System	IT	Ransomware
14	Outsider	Cybercriminal	Databases	IT and OT	Ransomware
15	Outsider	Cybercriminal	Databases, SCADA	IT and OT	Ransomware

TABLE 4. Defense Analysis.

#	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

926

List of Figures

927

1 (a) Traditional ICS systems; (b) Water system architectures; (c) Converged IT/OT

928

systems. 42

929

2 (a) The spiral attack model in converged IT/OT networks. The color coding matches

930

that of the zone division in Fig. 1c; (b) The diamond model of intrusion analysis,

931

with core (at the corners), meta- (light blue) and expanded meta-features (gray). . . 43

932

3 Matrix of defensible actions at each step of an attack. 44

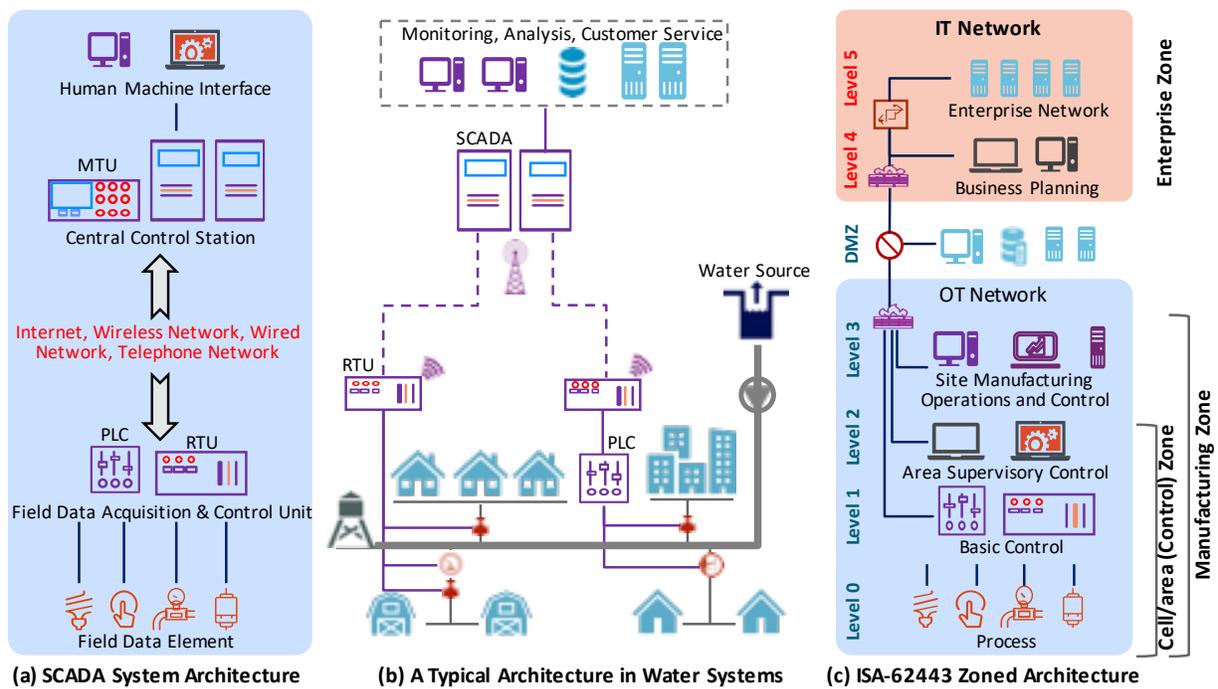


Fig. 1. (a) Traditional ICS systems; (b) Water system architectures; (c) Converged IT/OT systems.

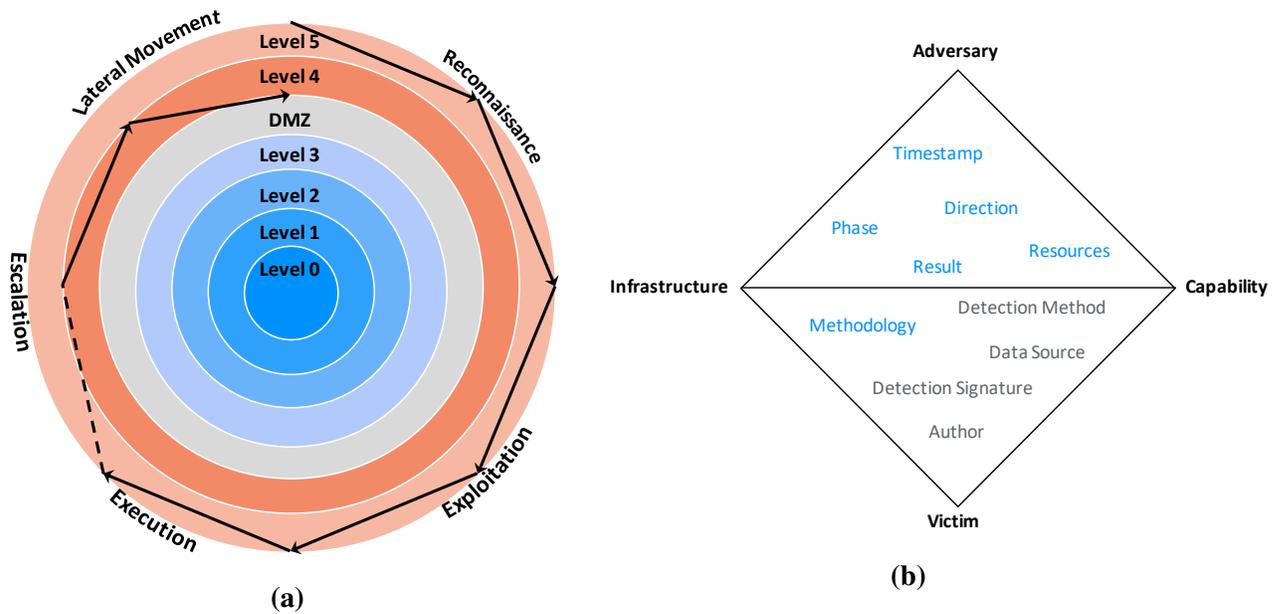


Fig. 2. (a) The spiral attack model in converged IT/OT networks. The color coding matches that of the zone division in Fig. 1c; (b) The diamond model of intrusion analysis, with core (at the corners), meta- (light blue) and expanded meta-features (gray).

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

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