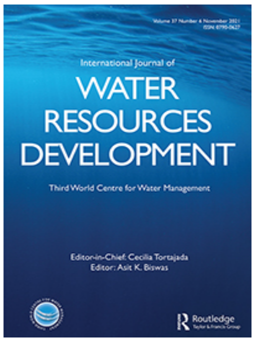

Routledge
Taylor & Francis Group

International Journal of Water Resources Development

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cijw20

Cybercrime, cybersecurity and water utilities

David Lloyd Owen

To cite this article: David Lloyd Owen (2021) Cybercrime, cybersecurity and water utilities, International Journal of Water Resources Development, 37:6, 1021-1026, DOI: 10.1080/07900627.2021.1965965

To link to this article: https://doi.org/10.1080/07900627.2021.1965965

Published online: 31 Aug 2021.

INTERNATIONAL JOURNAL OF WATER RESOURCES DEVELOPMENT
2021, VOL. 37, NO. 6, 1021–1026
https://doi.org/10.1080/07900627.2021.1965965

VIEWPOINT

Cybercrime, cybersecurity and water utilities

David Lloyd Owen

Envisager, Wales, UK

ABSTRACT
A total of 20 known cases of cybercrime attacks on water utilities have been seen in five countries between 2000 and 2021, with a steady increase in their frequency. The actual number of cyberattacks is higher, with 40 recorded in the United States in 2014–15. It is chiefly driven by organized crime and hostile state actors, along with disgruntled former employees. Vulnerabilities occur because of utilities adopting supervisory control and data acquisition (SCADA) systems without appropriate cybersecurity measures along with staff who have properly trained to be aware of phishing attacks. Threats such as these highlight the need for water utilities to have a comprehensive risk management system in operation.

ARTICLE HISTORY
Received 4 August 2021
Accepted 5 August 2021

KEYWORDS
Cybercrime; cybersecurity; water utilities; risk management; SCADA; vulnerability

What is cybercrime?

For water utilities, cybercrime is where external actors compromise the utility's operations by entering their control and data systems via the Internet. There are five main forms of cybercrime: (1) extortion by organized crime groups (they compromise the systems until paid by the utility): (2) corporate theft (stealing proprietary data for sale to third parties including organized crime groups); (3) groups seeking to make a point, showing they have breached a security system (perhaps getting rarer these days); (4) disgruntled former employees seeking revenge; and (5) state actors (Russia and China chiefly, along with Iran) or terrorism (mainly seen from groups based in the Middle East). For state actors, this is about damaging public trust and confidence in the utilities and therefore the government of the target country.

By its nature, all indications about where agents are located and who their intended targets are meant to be is open to dispute. There is a growing body of evidence that Russian-based groups are directing their efforts towards facilities in the United States, while others in China are focusing on Japan. Cybercrime takes place via single (often targeted) attacks or through advanced persistent threats, which are the approach favoured by state actors and terrorists.

Spear phishing is the chief approach, where an unsuspecting person working within the utility's network clicks on an infected link or opens an infected file and the malware enters the system. It is estimated that 90% of cyberattacks occur due to staff errors such as

CONTACT David Lloyd Owen david@envisager.co.uk

this. Phishing is most effective when messages are sent from a legitimate account, such as a supplier or trade association, that itself has been compromised. It is most effective when personalized emails are sent to identified recipients.

Watering hole domain attacks are based on identifying the websites a target regularly uses, and they infect these websites with malware which can then infect the target when the legitimate website us accessed by an unwitting user.

Denial-of-service attacks are the targeting of a site with such a volume of messages and data that the system is unable to function normally. This was a widely adopted approach by hacking and activist groups in the early days of the Internet. It has been seen less in recent years.

Why do we have cybercrime?

Cybercrime would not exist if it could not be carried out, or if there were no worthwhile gains from such an activity. It is evident that cybercriminals are often faced with an open door and significant damage or monetary gain can be obtained.

Water and sewerage utilities are targeted as part of a general attack on critical national infrastructure, especially by people working for, or on behalf of, hostile states. The Russian government has been targeting water utilities in the United States since 2018 (US C&ISA, 2018).

To date, the monetary cost of payments obtained by extortioners has been dwarfed by the cost of dealing with cybercrime. The more utilities are seen to pay extortioners, the more rewarding this approach will be seen to be. According to PwC (Williams, 2017), the typical utility holds US$65 million-worth of data of value to hackers. That is an incentive enough in itself.

The development of cybercrime

The first publicly known case of water utility-related cybercrime was in 2000. Information on a total of 20 cases is to some extent in the public domain as of June 2021. Of these, details have been revealed about 12 of them, with the rest providing minimal information about their location, let alone ownership. As Table 1 outlines, the frequency of identified cyberattacks on water utilities has consistently risen since 2000.

Most utilities are loath to publicize these attacks because of the damage it would do to customer trust as well as encouraging further attacks. For example, in the United States, the Department of Homeland Security (DHS) recorded 15 cyberattacks on water utilities recorded in 2014, rising to 25 in 2015, or 8.5% of cyberattacks recorded in the United

Table 1. Cyberattacks in the public domain, 2000–21.

Period	Cases	Countries/continents
2000–04	1	Australia
2005–09	2	USA
2010–14	3	USA
2015–19	8	USA (6), UK (1), Europe (1)
2020–21	5	USA (2), Israel (3)

Sources: Cyber Talk (2021); and Hassanzadeh et al. (2020).

States (Clark et al., 2016). Those 40 attacks compare with two which were in fact disclosed for that period. Likewise, 96% of cybercrime in Africa is either unnoticed or not reported (Serianu, 2017).

Examples of water utility cybercrime

These are some of the better-known examples of cybercrime (Clark et al., 2016; Cyber Talk, 2021; Hassanzadeh et al., 2020; Germano, 2019).

- A WWTW in Maroochy Shire, Queensland, Australia, was hacked in 2000 resulting in the discharge of 800 m^3 of raw sewage into rivers and parkland. The attack was carried out by an ex-employee of the firm who had installed the utility's supervisory control and data acquisition (SCADA) in 48 separate attacks over two months, which were designed to appear as pumping faults.
- In 2016, Lansing Board of Water and Light in the United States was attacked via a spear phishing operation. Accessing the commercial network, the cybercriminals locked the utility out of its own systems. The utility paid US$25,000 in Bitcoin to regain access. Replacing the infected computers and software cost US$10 million with a further US$2.4 million in remediation costs.
- Also in that year, a vulnerability in a remote wireless Internet connection and a hard-coded factory password allowed hackers to attack an unnamed water utility's industrial control system for two months. Patches has not been installed and firmware was not updated. There was no scanning for intruders. Sticking with a standard password also does not help.
- A US water utility (still unnamed) was hacked in 2017 by a Syrian group that was able to manipulate its chemical dosing for a limited period of time.
- In January 2020, Greenville Water in the United States announced it had suffered a targeted cyberattack that affected online payments for the 500,000 people it served. That month, customer-sensitive information from 300 accounts at Detroit Water & Sewerage Department in Michigan was exposed due to a breach.
- In 2021, a water treatment plant in Osmar, Florida in the United States was hacked, and the hacker was able to raise sodium hydroxide levels for a brief period. It was noted by an operator who remedied the situation before it could cause any significant harm. In this case, TeamViewer (remote access for information technology (IT) systems) software had been replaced by a more advanced and secure tool, but had been left on the system, allowing a 'front door' attack.

Where the vulnerabilities are

With the exception of rogue ex-employees, most, if not all of these attacks could have been prevented with appropriate cybersecurity measures. There is a need to effectively blend traditional (pre-digital) control systems with IT in a secure manner, since if this is not done, potential insecurities can be opened up.

One of the chief vulnerabilities to emerge is when layers of technology are placed on top of each other without due consideration as to how these will affect cybersecurity. For example, according to Bluefield, 79% of US community water systems have SCADA systems, but just 21% have network optimization allowing remote management. Traditional SCADA units were not linked to strategic decision systems, because they could not transmit the data required. Newer SCADA systems are designed for integration and so it is essential that any potential vulnerabilities are addressed.

Staff training and management awareness is too often taken for granted. Where smaller utilities predominate, the lack of consolidation means a lack of resources and experience. The entire essence of cyberattacks it to exploit every possible opening, every lapse in vigilance leading to a vulnerability being exposed when a link is clicked open.

In the case of water and wastewater, larger utilities may well have a lot of sites relative to their staff and revenues, although central staffing may be strong. Smaller utilities will often have limited trained staff and protection technology. While UK water utilities are obliged to be cybersecure, just 10% of companies currently have a formal cyber security plan.

Another potential vulnerability could be via smart domestic water meters and Internet-enabled accounts, which unless suitably firewalled could provide an entry into a utility's systems. Finally, as remote metering and monitoring devices are deployed in the field and in networks, these could perhaps provide a new route to hack into these.

The Internet of Things (IoT) opens up a new area of potential vulnerability. Where large numbers of cheap monitoring and communicating devices with poor protection (a standard password, for example) are networked, this creates the potential for massive interlinking of information flows, one of which could be compromised. Likewise, remote working (working from home) also opens up new potential vulnerabilities if adequate precautions are not made to ensure that remote staff are not using compromised digital devices.

Making utilities cybersecure

Under a plan enacted in 2017 (DEFRA, 2017), the UK water utilities are meant to be fully secure by 2021. In addition, the 2018 General Data Protection Regulations (GDPR) make UK utilities liable for heavy fines if they do not demonstrate that they have made their customer data secure. In the United States (Germano, 2019), the 2018 Water Infrastructure Act obliges utilities serving more than 3300 people to carry out a risk and resilience assessment, which has to be recertified every five years.

The ISO-27001 standard is a useful starting point for utilities. This governs the specification for an information security management system (ISMS). ISO-27001's best-practice approach helps organizations manage their information security by addressing people and processes as well as technology.

In practice, this means that all staff need to be trained to appreciate that they are in the firing line. The overriding need is to establish a cybersecurity culture based on technology, staff and physical protection (location of IT equipment). Utilities need to systemically remove all devices that are no longer being supported by the manufacturer, while all software and systems need to be updated for all vulnerabilities and threats. All the vendor default security settings have to be changed as a matter of course.

A first measure is to segment operational units so that if one treatment works is infected, this will not spread to others. Here, unidirectional gateways are ideal as they allow data to be transmitted from a protected network but prevent the transmission of information from outside the system back to the protected network. Within utility networks, secure zones can be established with virtual local area networks. True isolation has been established between, for example, a water treatment works and the corporate IT system allowing the water treatment works to transmit data to the corporate system. These require time and money (US$300,000 per corporate system) to establish, configure and test and two to three days per week of trained staff time to maintain.

Smaller utilities can use virtual routing and forwarding which allow networks to be virtually segmented without the need for multiple devices. In addition, domestic-grade equipment (routers, etc.) are no use even for small utilities. In addition, regular (daily, for example) back-ups can make data encryption attacks ineffective once the malware has been removed.

Implications for water and wastewater utilities

Indications are that a secure system will cost at least US$300,000 for hardware and a minimum of two to three days per week of staff support to create the basis of a secure system. On top of this are the costs of staff training, active data backing up and ancillary actions. This points to operating costs in the region of US$10,000–20,000 per annum and appreciably more for large utilities with complex networks.

In the United States, there were 43,742 water systems serving fewer than 3300 people in 2010, serving 29.5 million people. A further 4914 systems (28.6 million people) served 3300–10,000 people. These systems would be hard pressed to afford full security with secure zones and dedicated staff. For large (*n* = 3,801,108.5 million people) and very large (*n* = 416,138.1 million people) systems, effective security would be expected.

One approach would be to consolidate separate systems into a secure network. We are seeing low key moves in this direction. For example, Sciens Water (US, private equity) owns 16 utilities, which in turn control 293 water systems. This creates a platform where economies of scale can be established. Large numbers of systems and utilities create large numbers of potential vulnerabilities, which redoubles the need for truly effective cybersecurity.

The scope for cybersecurity as a force for consolidation is strong, even if consolidation in reality remains a slow process. It appears to be taking place most effectively through incremental acquisitions of adjacent assets or concessions (Greece, Italy, United States), building up a portfolio of assets or concessions (United States, France, Spain), the development of a portfolio of small utilities and systems (United States), of the merger of substantial companies (England and Wales). In every case, progress is being measured in decades, not years.

It is evident that small utilities (and systems) that are not part of an integrated network of utilities are going to struggle to afford any effective form of cybersecurity. Their main hope will be that they are too small to be of interest to cybercriminals. That is a risky assumption to make.

Cybersecurity and utility resilience

Water utilities are facing unprecedented challenges. In the past decade, climate change and cybercrime have emerged as new threats and, more recently, are the implications of Covid-19. These challenges have one crucial element in common: while until recently, none of them was of a concern, they now pose existential threats. The conservative, reactive utility will be severely pressed to carry on in the face of these challenges. Those utilities that can face these will do so by developing a full understanding of their own activities and their vulnerabilities. That, in turn, will place them in good stead when it comes to meeting any new and for now unforeseen threats they may face.

Disclosure statement

No potential conflict of interest was reported by the author.

ORCID

David Lloyd Owen http://orcid.org/0000-0002-2094-9008

References

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2016). *Protecting drinking water utilities from cyber threats*. Idaho National Laboratory. https://www.osti.gov/pages/servlets/purl/1372266

Cyber Talk. (2021, June 17). Poisoned water? Cyber criminals cause concern in California. https://www.cybertalk.org/2021/06/17/poisoned-water-cyber-criminals-cause-concern-in-california/

DEFRA. (2017). *Water sector cyber security strategy*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/602379/water-sector-cyber-security-strategy-170322.pdf

Germano, J. H. (2019). *Cybersecurity risk & responsibility in the water sector*. AWWA. https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020, January 25). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering*, *146*(5), 03120003. https://doi.org/10.1061/(ASCE)EE.1943-7870.0001686

Serianu. (2017). *Africa cyber security report, 2017*. https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

US C&ISA. (2018, March 15). *Alert (TA18-074A) Russian government cyber activity targeting energy and other critical infrastructure sectors*. US Cybersecurity & Infrastructure Security Agency. https://us-cert.cisa.gov/ncas/alerts/TA18-074A

Williams, A. (2017, January 1). *Cyber security: How water utilities can protect against threats*. WWi. https://www.waterworld.com/international/utilities/article/16201183/cyber-security-how-water-utilities-can-protect-against-threats