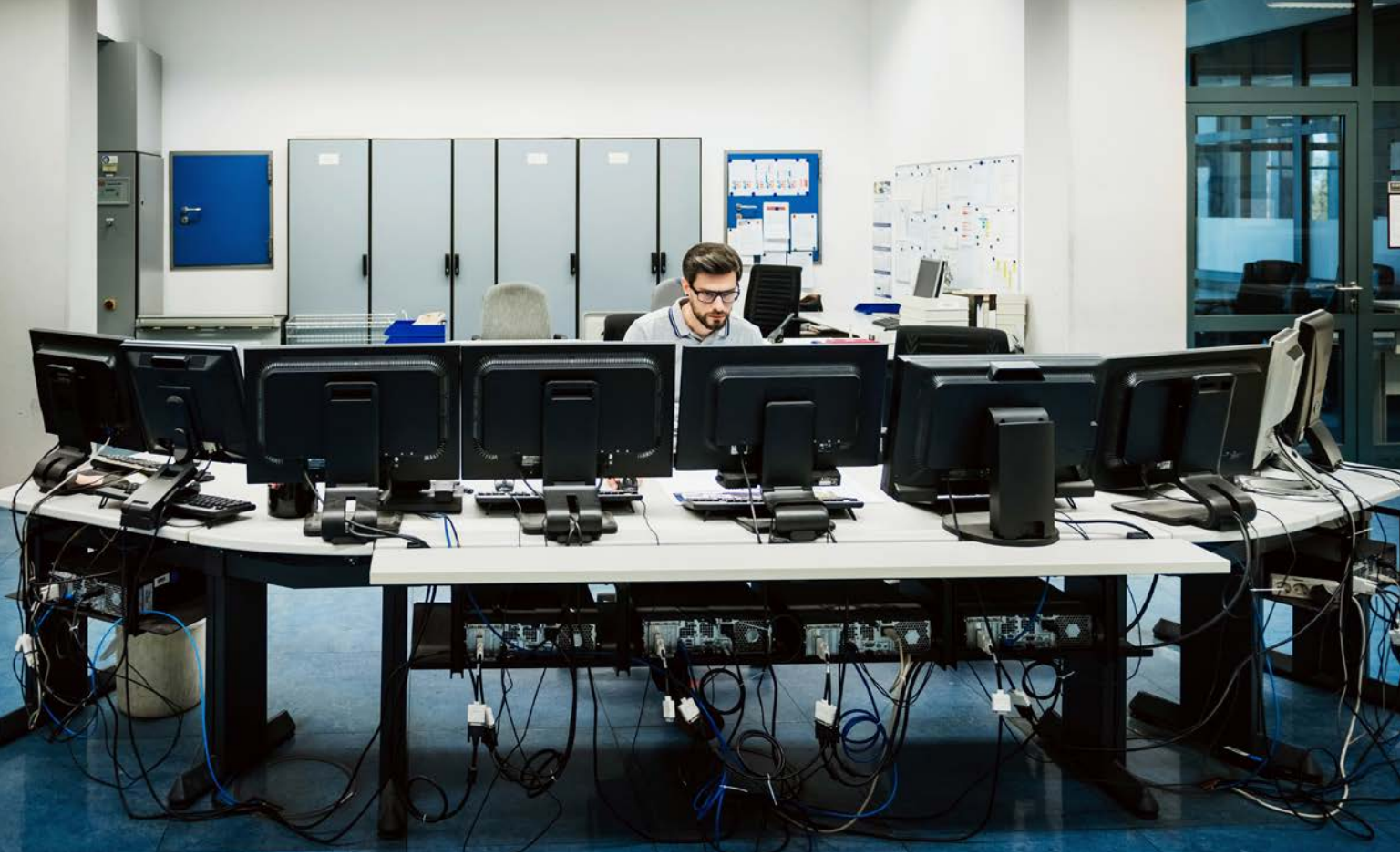


How cyber-secure is your utility?

The threats are serious — take advantage of resources to protect your systems

Charles Egli

Imagine this: It is a typical morning at a water resource recovery facility when calls start pouring in from upset customers and public officials. They are complaining about wastewater backups across the city's downtown.

The control center supervisor checks the process control interface and everything appears normal. Indicators show the treatment system, pumps, and lift stations all humming along correctly as usual. The maintenance director sends crews to investigate. A few hours later they discover a vital lift station is off-line, despite what the process control system screens portray.

Two weeks later, and with the help of cybersecurity experts, the facility discovers its industrial control system was hacked. The attackers sped up the lift station's pumps, burned out machine parts, and manipulated the process control system's human–machine interface to disguise what they had done, delaying system restoration.

After further review, investigators trace the intrusion back to one employee who responded to an email allegedly from a utility supervisor. The email asked for login credentials. The employee had replied quickly, not realizing it was a phishing scam designed to trick him into sharing sensitive information.

Ultimately, investigators could not determine the identity of the hackers, but it is clear their strike was highly sophisticated and caused a lot of damage. In addition to operational downtime, the utility had to foot the bill for cleaning up buildings that experienced backups, repairing the damaged pump, and restoring system software. The event also eroded public opinion about the utility's reputation and its management. It would take years to rebuild the trust of the local community and civic leaders.

Fortunately, this particular phishing scam is fiction – for now. Current research reveals critical U.S. infrastructure is not adequately prepared for cyberattacks.

◀ **Industrial control systems allow for processes to be automated and regulated and monitored remotely, but also present vulnerabilities.**

October is National Cybersecurity Awareness Month

This monthlong recognition is a collaborative effort between government and industry to ensure individuals and businesses have the resources they need to stay safer and more secure online. It serves as an essential reminder to examine your facility's cybersecurity and learn about resources available for water resource recovery utilities.

To help foster this work, the U.S. water and wastewater sector's leading national associations and research foundations established the Water Information Sharing and Analysis Center (WaterISAC) in 2002, in coordination with the U.S. Environmental Protection Agency. That same year, it was authorized by Congress in the Bioterrorism Act. WaterISAC is the designated information sharing and operations arm of the Water Sector Coordinating Council.

National Cybersecurity Awareness Month

While many utilities in the water sector have invested heavily in cybersecurity, many others have a way to go.

This observation fits with the *M-Trends 2018* report produced by cyber experts at Mandiant Consulting, a FireEye company. The report states that among other shortcomings, many organizations struggle to implement security risk management functions, harden authentication and authorization controls, and operationalize cyber threat intelligence into detection and response capabilities.

The government also is sounding the alarm. "Cyberattacks are one of the highest risks facing water and wastewater facilities today," Peter Grevatt, director of the Office of Ground Water and Drinking Water at the U.S. Environmental Protection Agency recently declared. "Hackers can steal valuable customer and employee data, and disable business enterprise and process control systems. All water and wastewater utilities should adopt best practices for cybersecurity and be prepared to recover from a cyberattack."

Cybersecurity leaders are becoming increasingly concerned about what the future may hold for U.S. critical infrastructure. In a June 2018 survey conducted by the organizers of the renowned Black Hat security conferences, nearly 70% (up 10% from 2017) of cybersecurity specialists and researchers believe that a successful cyberattack on U.S. critical infrastructure will occur in the next 2 years.

The attackers

WaterISAC has observed that the number and sophistication of adversaries seeking to exploit critical infrastructure vulnerabilities are growing. So, who are these adversaries? And how are they orchestrating their attacks? And why are they doing this? Figure 1 (right) provides a quick snapshot, which is discussed in more detail below.

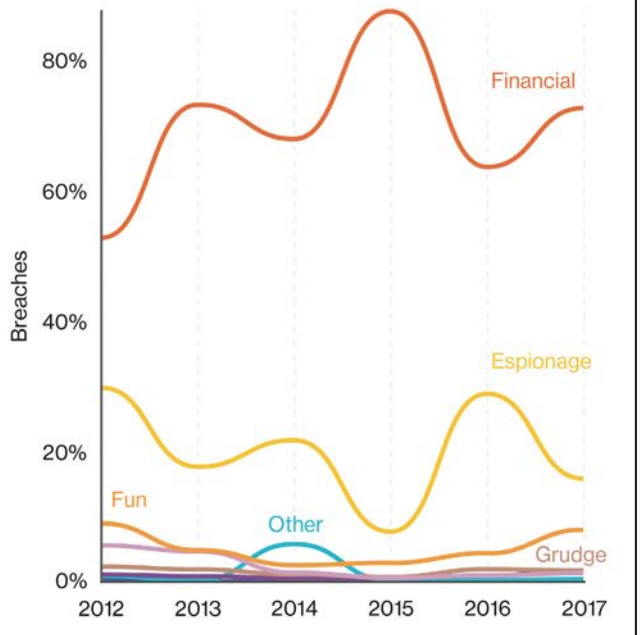
Nation–States

These are among the most formidable of adversaries. In mid-February, the U.S. Senate Intelligence Committee received its annual briefing on worldwide threat assessment from the U.S. intelligence community. At the briefing, Director of U.S. National Intelligence Dan Coats and other U.S. intelligence community leaders warned about cyber threats from Russia, China, Iran, and North Korea. According to the assessment, both nation-states and malign actors are becoming "more emboldened and better equipped in the use of increasingly popular cyber toolkits. The risk is growing that some adversaries will conduct cyberattacks – such as data deletion or localized and temporary disruptions of critical infrastructure – against the United States in a crisis short of war."

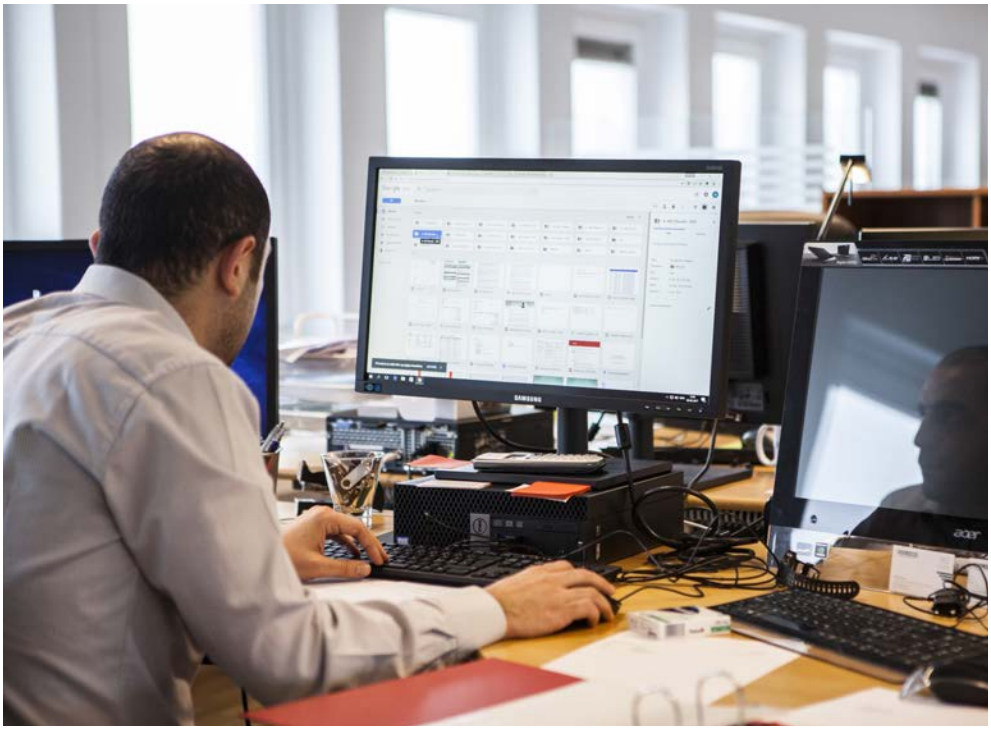
Russian government cyber actors are responsible for recent assaults against the U.S., including the water sector. "The Administration is confronting and countering malign Russian cyber activity, including their … destructive cyberattacks, and intrusions targeting critical infrastructure," said U.S. Treasury Secretary Steven Mnuchin during a March 15, 2018, press conference. That same day, the U.S. Department of Homeland Security (DHS) released Technical Alert 18-074A, which reports on "indicators of compromise and technical details on the tactics, techniques, and procedures used by Russian government cyber actors on compromised victim networks."

Iran also has targeted the water sector. This year, the FBI issued an alert about the Mabna Institute, a company working on behalf of the Iranian government to illegally gain access to non-Iranian scientific resources through computer intrusions. The group gained entry into the computer systems of U.S. organizations via "password spray attacks," a tactic that involves attempting a single password against a population of accounts before moving to a second

Figure 1. Threat-actor motives in breaches



Verizon 2018 *Data Breach Investigations Report.*



Employees can become unwitting accomplices in cybersecurity breaches. Pexabay.com

password. Although not identified in the FBI's original alert or the indictment of the Iranian individuals associated with the Mabna Institute, WaterISAC has learned that this activity targeted drinking water and water resource recovery utilities.

Financially motivated cyber criminals

Verizon's *2018 Data Breach Investigations Report (DBIR)* reveals that financial motives were behind some 70% of cyber breaches in 2017 with criminals frequently deploying ransomware or crypto-mining malware. Physical threats also might be applied to induce ransom payments. For example, a team of researchers at the Georgia Institute of Technology developed a ransomware variant that could allow a hacker to migrate into an industrial control system and alter the amount of chlorine fed into a water supply system. Unless a utility has fully backed up its data, a threat to public health such as this could spur managers to meet the demands of criminals.

Revenge seekers

In other cases, a perpetrator may seek revenge for a perceived injustice. According to Verizon's *DBIR*, individuals who harbor grudges against their targets perpetrate 5% of cyberattacks. In fact, an individual holding a grudge performed an infamous case of a successful cyberattack on a water resource facility. In 2000, a rejected job application motivated a man to hack Maroochy Water Services in Queensland, Australia. Using a stolen wireless radio, a SCADA controller, and control software, the man released 800,000 L (211,300 gal) of wastewater into local parks, rivers, and even the grounds of a Hyatt Regency hotel. Cleaning up the spill and its effects took days and required the deployment of considerable resources. Marine life died, and residents reported the stench was unbearable.

Anyone can purchase a cyber weapon

It may be surprising to learn that malicious actors with technical expertise did not necessarily perform the types of attacks cited in this article. Today, all it takes is the right connections to go online and buy malware and vulnerability information from savvy criminal entrepreneurs. Many of the online marketplaces for this kind of activity exist on the Dark Web, an area of the World Wide Web where the servers of websites are hidden, providing anonymity to users and administrators. One can purchase ransomware, spyware kits, and other advanced online threats priced from $39 to $10,000, depending on the level of sophistication required.

The Dark Web is a convenient point of entry for a variety of cyber criminals. For example, Shadow Brokers, a mysterious group of hackers who stole computer disks full of U.S. National Security Agency secrets in 2013, used the Dark Web to distribute some of the agency's secret cyberattack tools. These tools included the "EternalBlue" exploit, which was used to help orchestrate the infamous "WannaCry" ransomware campaign that has infected company networks across 150 countries and hundreds of thousands of computers.

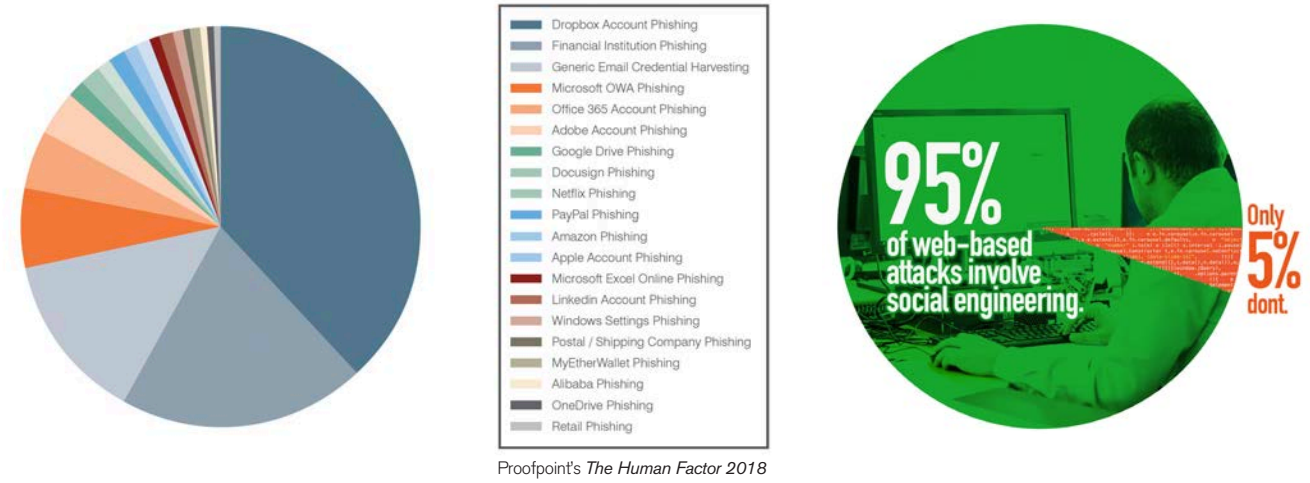
Social engineering and phishing

Through social engineering, cyber criminals also may get inadvertent assistance from employees of the organization they intend to attack. Attackers can use deception to solicit sensitive information from unsuspecting employees. The most common method is phishing. A malicious actor sends a computer user a seemingly legitimate email, but by clicking on a malicious attachment, visiting a malicious website, or replying to the email, the employee discloses sensitive account and login information. According to *The Human Factor 2018, a* report by the cybersecurity company ProofPoint, as many as 95% of web-based attacks now incorporate social engineering. Phishing campaigns are becoming more and more convincing. This makes social engineering an effective way for threat actors to gain entry into an organization's systems. Figure 2 (p. 43) gives a breakdown of where phishing attacks happened in 2017.

Third-party systems

In another type of attack that leverages privileged access, an attacker compromises some component in an organization's supply chain, such as a contractor or vendor that provides goods or services. The 2013 breach of the retailer Target was facilitated via such means, specifically through an HVAC contractor servicing some of the stores.

Figure 2. Relative email message volume for the top 20 phishing lures in 2017



Proofpoint's *The Human Factor 2018*

Social engineering is an effective way for threat actors to gain entry into an organization's systems.

Attackers also are using these methods against more than just the retail sector, including sectors that depend upon industrial control systems. Earlier this year, numerous major natural gas pipelines experienced data system blackouts after a cyberattack on a third-party vendor's electronic communications system. Interviewed by *Threatpost* magazine in the aftermath of those incidents, Bryan Singer, director of security services at the cybersecurity provider IOActive said, "In probably three-quarters of the cases where a hacker is targeting an industrial control system, a very common pattern we see is entrance through vulnerable, third-party systems."

Helpful resources

The water sector's official information sharing resource

Since its inception, WaterISAC has assisted drinking water and water resource recovery utilities bolster their physical and cybersecurity and recover from disasters. It is a clearinghouse of cybersecurity resources. Members receive alerts on information technology and industrial control system threats and vulnerabilities tailored to the needs of the water sector.

One of WaterISAC's most popular resources is its *10 Essential Cybersecurity Measures for Water and Wastewater Utilities*. (See sidebar, right.)

The list provides an overview of fundamental industrial control and enterprise system security measures, accompanied by hyperlinked references to trusted resources from the private sector and government.

WaterISAC collects cyber incident reports from members, looks for patterns, advises members about malicious activities to look out for, and recommends remedial actions. Each month, WaterISAC also hosts cybersecurity web briefings led by experts from the federal government, private firms, and WaterISAC analysts. Members learn about the latest threats and can interact directly with the presenters.

Automated threat monitoring

Information on cyber incidents and threats amount to a daily deluge of data, much of it very technical. Several utilities rely on automated threat monitoring, whereby a third party scans network traffic for malicious activity or anomalies indicating a possible breach. To help its members manage all of this information, WaterISAC has formed a partnership with the cybersecurity

WaterISAC's 10 essential cybersecurity measures

1. Inventory all networked devices and assess risks.
2. Implement network segmentation technologies to eliminate external exposure.
3. Use only secure remote access solutions.
4. Enhance role-based access controls and implement system logging and auditing.
5. Use long, memorized passwords and change default passwords.
6. Maintain awareness of vulnerabilities and apply necessary patches.
7. Develop and enforce policies on mobile and Internet-of-Things devices.
8. Implement a cybersecurity awareness program and deter insider threats.
9. Involve executives in cybersecurity.
10. Implement measures for detecting and responding to compromises.

Director of National Intelligence Dan Coats and other intelligence community leaders testifying on worldwide threats before the U.S. Senate Intelligence Committee. Office of the Director of National Intelligence

firm Perch Security. Perch's platform monitors incoming and outgoing network traffic and compares it against WaterISAC's threat repository to identify suspected indicators of compromise. The repository incorporates threat intelligence from two U.S. Department of Homeland Security cyber intelligence programs as well as private sector intelligence. If Perch detects threats in a utility's traffic, it alerts the utility to take action.

AWWA and NIST

The American Water Works Association (AWWA; Denver) and the National Institute of Standards and Technology (NIST; Gaithersburg, Md.) also offer helpful information. AWWA Cybersecurity Guidance provides a "consistent and repeatable recommended course of action to reduce vulnerabilities to cyberattacks." The AWWA Cybersecurity Tool complements the guidance by allowing utilities to evaluate their current environment through selected use cases that mirror their organization's operations.

The AWWA products are the foundation for a water sector-specific approach for adopting the NIST Cybersecurity Framework, which is voluntary guidance centered on consensus-based cybersecurity standards and practices. The framework has received the widespread endorsement of industry and government.

www.awwa.org/cybersecurity
www.nist.gov/cyberframework

U.S. Environmental Protection Agency (EPA)

The EPA Water Security Division's *Cybersecurity Incident Action Checklist* provides a list of tasks that utilities and their IT vendors should conduct to prepare against compromises. It also includes links to other helpful resources.

www.epa.gov/waterutilityresponse/incident-action-checklists-water-utilities

Free DHS cybersecurity preparedness assessments

DHS also has free, voluntary cybersecurity assessment programs that drinking water and water resource recovery facilities have found very helpful. In fact, the water sector has been among the most active of all critical infrastructure sectors in taking advantage of these assessments.

DHS offers eight types of evaluations, beginning with the high-level Cyber Resilience Review, which examines an organization's operational resilience and the cybersecurity practices of its critical services. Other assessments address external dependencies management, system architecture and configurations, and more. DHS personnel perform the evaluations at the utility and in collaboration with utility staff.

www.us-cert.gov/ccubedvp

Take the initiative

Many cybersecurity analysts say it is not a question of *if* an organization will suffer a breach, but rather *when* it will happen – that's a compelling call to action. While the challenge of cybersecurity is immense, incident post-mortems often reveal that a simple cybersecurity measure was ignored or overlooked and eventually exploited. Even nation–states, with all their advanced capabilities, often use popular and unsophisticated tools and methods to invade their targets.

WaterISAC urges all utilities to take the time to implement cybersecurity measures and work with government, association, and business partners to assess the effectiveness of their efforts. When so much information is readily available about potential threats and how to prevent them, water resource recovery facilities have more resources than ever before to thwart cyberattacks.

Charles Egli *is the lead analyst at WaterISAC, based in Washington, D.C., providing analytical, preparedness, and operational support of water sector security. He is also a U.S. Navy Reserve officer.*