Cybersecurity Risk & Responsibility in the Water Sector

Prepared by Judith H. Germano

American Water Works Association

Dedicated to the World's Most Important Resource®

Cybersecurity Risk & Responsibility in the Water Sector

Prepared by
Judith H. Germano

Contents

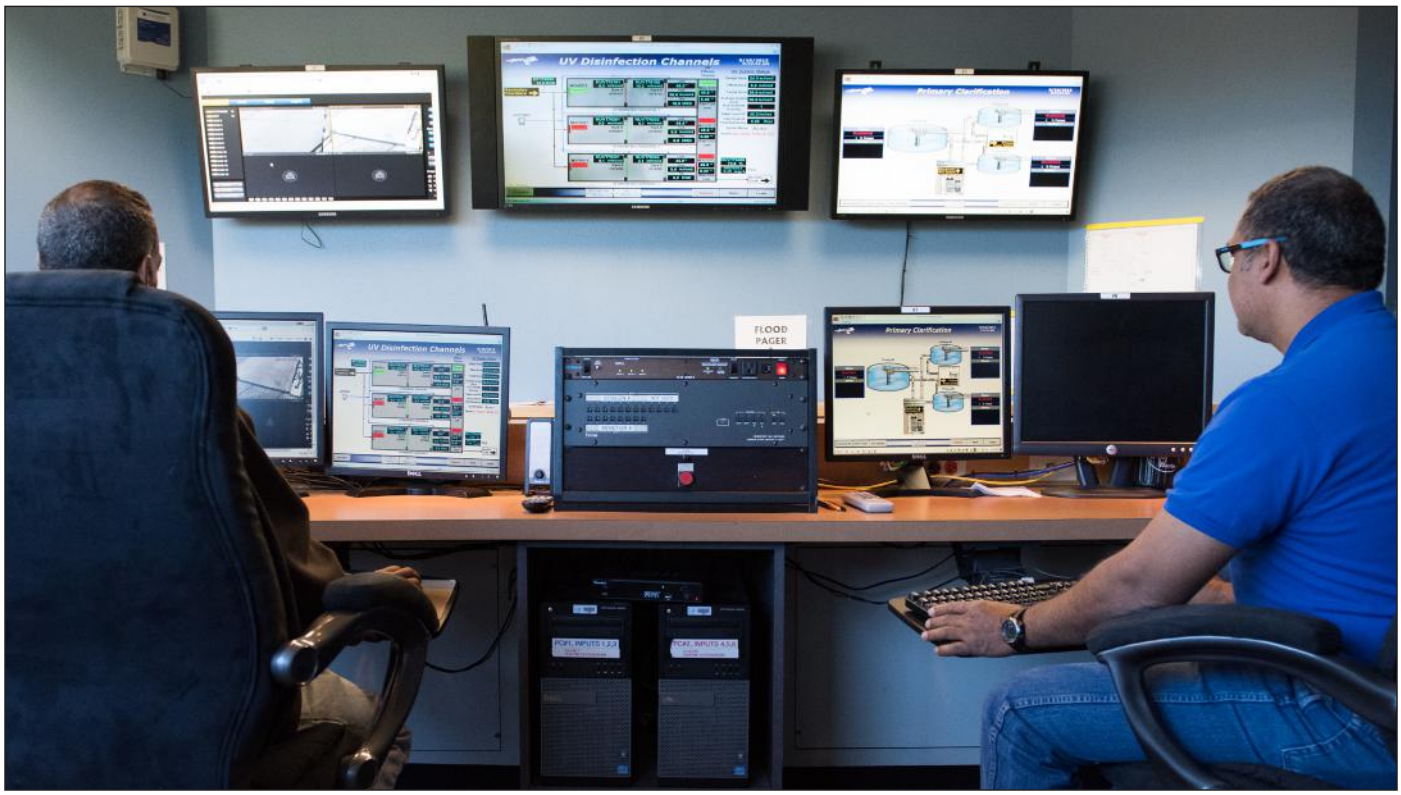
ACKNOWLEDGEMENTS

Judith H. Germano is a Professor and Distinguished Fellow at the NYU Center for Cybersecurity, teaching incident response, cybercrime and emerging threats in NYU's Masters in Cybersecurity Risk and Strategy executive education degree program, and is an Adjunct Professor of Law at NYU School of Law. Judith is the founder of Germano Law LLC, advising organizations and corporate boards on cybersecurity, data privacy, fraud and regulatory compliance issues. Judith is the former Chief of Economic Crimes at the U.S. Attorney's Office for the District of New Jersey; a federal prosecutor for 11 years, Judith has handled matters of cybercrime, identity theft, securities and other financial fraud, political corruption and national security.

AWWA would like to thank multiple reviewers including Mike Hooker, Robert Walters, Patrick Norton, John Lucas, and Jaimie Foreman.

Project Funding

This project was funded by the American Water Works Association (AWWA), utilizing Water Industry Technical Action Fund (WITAF), as WITAF Project #030 and managed by Kevin M. Morley.



Disclaimer

The authors, contributors, editors, and publisher do not assume responsibility for the validity of the content or any consequences of its use. In no event will AWWA be liable for direct, indirect, special, incidental or consequential damages arising out of the use of information presented herein. In particular, AWWA will not be responsible for any costs, including, but not limited to, those incurred as a result of lost revenue.

EXECUTIVE SUMMARY

Cybersecurity is a top priority for the water and wastewater sector. Entities, and the senior individuals who run them, must devote considerable attention and resources to cybersecurity preparedness and response, from both a technical and governance perspective. Cyber risk is the top threat facing business and critical infrastructure in the United States. Government intelligence confirms the water and wastewater sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign, and individual criminal actors and groups threaten the security of our nation's water and wastewater systems' operations and data. Managing cybersecurity is a complex challenge that requires an interdisciplinary, risk-based approach, involving an organization's business leaders, as well as their technical and legal advisors.

A robust and tested cybersecurity program is critical to protect public health and safety, prevent service disruptions, and safeguard customer and employee personal and financial information. Inadequate cybersecurity measures and flawed responses to cybersecurity incidents carry tremendous risk. In addition to serious threats to people, property, operations and data, cybersecurity incidents also can result in potential civil and regulatory liability, and reputational harm. Attacks will happen; do not be caught unprepared.

Steven D. Shirley, Executive Director of the National Defense Information Sharing and Analysis Center™ (NDISAC™)

Despite sector challenges, it is critically important to bolster cybersecurity protocols and defenses. Getting cybersecurity "right" is not an easy issue. Threats are persistent and mutable. The diverse nature of the water and wastewater sector, with organizations of varying size and ownership, the sector's splintered regulatory regime, and a lack of cybersecurity governance protocols, present significant cybersecurity challenges.

Moreover, entities within the sector often face insufficient financial, human and technological resources. Many organizations have limited budgets, aging computer systems, and personnel who may lack the knowledge and experience for building robust cybersecurity defenses and responding effectively to cyber attacks.

Despite these challenges, organizations—on their own and with outside technical and legal experts as needed—must develop a plan and give sufficiently rigorous attention to cybersecurity. An optimistic reliance on sovereign immunity defenses or insurance policies, or an unconfirmed expectation that someone else within the organization is "handling" cybersecurity issues, are not sufficient to protect an organization or its leaders from the repercussions of a cybersecurity attack and the related reputational harm.

There are scalable and effective measures that water sector members—individually and collectively—can take to improve the cybersecurity of their organizations, and of the sector as a whole. Given the very real threat and significant consequences of a cyber attack, it is critical that organizations prioritize cybersecurity and take reasonable steps to prevent, detect and respond to cyber incidents.

CYBER RISK: A TOP THREAT, CYBERSECURITY: A TOP PRIORITY

Significant Risk

Cyber risk is the top threat facing business and critical infrastructure in the United States, according to the Director of National Intelligence, the Federal Bureau of Investigation and the Department of Homeland Security.[1] A survey of more than 20,000 utility employees revealed that cyber threats are what they fear could have the biggest impact on operations, with a lack of resources and conflicting priorities as the greatest challenges.[2] Water and Wastewater Sector (referred to collectively here as "water sector") entities have suffered a range of attacks, including from ransomware attacks, tampering with Industrial Control Systems, manipulating valve and flow operations and chemical treatment formulations, and other efforts to disrupt and potentially destroy operations. In March and April 2018, the U.S. Department of Homeland Security and Federal Bureau of Investigation warned that the Russian government is specifically targeting the water sector and other critical infrastructure sectors as part of a multi-stage intrusion campaign.[3] Attacks for financial, political and terroristic gain are a serious concern.

The effects of a cybersecurity attack on critical water sector operations could cause devastating harm to public health and safety, threaten national security and result in costly recovery and remediation efforts to address system issues as well as data loss. Attacks causing contamination, operational malfunction, and service outages could result in illness and casualties, compromise emergency response by firefighters and healthcare workers, and negatively impact transportation systems and food supply. Water sector entities also are responsible for protecting sensitive personal information, including employee records and customer billing data. This personal information is an attractive target for cybercriminals and the stolen data business continues to grow. Indeed, the U.S. had 16.7 million identity fraud victims in 2017, with $16.8 billion stolen from U.S. consumers through identity fraud.[4]

---

[1] *https://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx.*

[2] *BRIDGE Energy Group, 2018 BRIDGE Index™ Utility Industry Grid Operations Survey, Jan. 9, 2018, https://www.bridgeenergygroup.com/news/press/bridge-energy-groups-2018-utility-industry-survey-grid-operations/.*

[3] *U.S. Department of Homeland Security (DHS), US-CERT, Alert (TA18-074A), Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, March 15, 2018, revised, March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A; U.S. DHS, US-CERT, Alert (TA18-106A), Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, April 16, 2018, revised, April 20, 2018, https://www.us-cert.gov/ncas/alerts/TA18-106A.*

[4] *Javelin Strategy and Research, 2018 Identity Fraud Study, February 6, 2018, https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.*

Examples of confirmed water sector attacks include, among others:

- City of Atlanta ransomware attack. The City of Atlanta was crippled by a ransomware attack in March 2018, which disrupted city utilities, courts and other operations.[5] For roughly a week, employees with the Atlanta Department of Watershed Management were unable to turn on their work computers or gain wireless internet access, and two weeks after the attack Atlanta completely took down its water department website "for server maintenance and updates until further notice."[6] It has taken Atlanta months, and estimated costs of up to $5 million in recovery efforts, to address the attack.[7] (While the Atlanta attack focused primarily on public-facing operations, the Colorado Department of Transportation was hit with a sequence of ransomware attacks on its back-office systems, costing approximately $1 to $1.5 million to address.[8])
- Ransomware attack on a water utility effected through spear-phishing. An employee clicked on a malicious email link that caused malware to download. Cybercriminals gained access through an Internet-facing commercial network and locked the utility out of its own systems, demanding the equivalent of $25,000 in Bitcoin to recover access.[9] Replacing the infected computers and software cost $10 million, and full remediation costs (including paying the ransomware in this instance) were approximately $2.4 million, $500,000 of which was not covered by insurance.[10] This attack underscores the importance of resiliency and redundancy of systems, malware detection and prevention, and employee training, as well as the importance of having cyber-insurance in place.
- Attack on Industrial Control System (ICS) of a water and sewage authority. Cybercriminals exploited a vulnerability in a remote wireless Internet connection for operations for approximately two months, and also exploited a hard-coded factory password. [11] This attack underscored the importance of staying current with vendor patches and firmware updates, and regularly (if not continuously) scanning networks for intruders. It also highlights a common developer flaw of hard-coded passwords, which should be avoided if possible; if the password is for the initial default account, that account should be deleted after the set-up.[12]
- In one water utility attack, cybercriminals exploited antiquated computer systems to gain access to valve and flow operations and were able to manipulate the water flow and amount of chemicals used to treat the water. Cybercriminals also accessed customer data via the company's online payment system, through which the attackers gained administrator credentials and maneuvered laterally through the network.[13]

---

[5] *https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html.*

[6] *"https://www.reuters.com/article/us-usa-cyber-atlanta-water/atlanta-takes-down-water-department-website-two-weeks-after-cyber-attack-idUSKCN1HC2WB.*

[7] *https://www.ajc.com/news/local/atlanta-network-almost-recovered-from-cyber-attack-cost-still-unkown/k6srGim85Q8dKwUFPbcDhN/.*

[8] *https://statescoop.com/colorado-has-spent-more-than-1-million-bailing-out-from-ransomware-attack.*

[9] *https://thehackernews.com/2016/04/power-ransomware-attack.html.*

[10] *https://www.freep.com/story/news/local/michigan/2016/11/09/bwl-paid-ransom-cyberattack/93576218/.*

[11] *See, e.g., https://www.csoonline.com/article/3038302/application-development/hard-coded-passwords-remain-a-key-security-flaw.html.*

[12] *See Id.*

[13] *See Verizon's Data Breach Digest (2016) p. 39-42.*

- In the well-publicized Bowman Dam hack, Iranian activists exploited a vulnerability to identify an unprotected computer that controlled sluice gates and other functions of the dam. The hactivists detected the vulnerability through "Google Dorking," a process of performing advance Google searches to detect vulnerabilities. At the time of the attack, the gate was manually disconnected for maintenance, which helped avoid more serious harm. Remediation costs for the dam exceeded $30,000, and the hackers were charged in a criminal indictment.[14] The relatively simple way the hackers discovered the significant vulnerability underscores the importance of regular security assessments and penetration testing of systems, networks and applications.

In a March 2018 technical alert, DHS and FBI warned of "a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS)." The alert warns the water sector also is a target of this Russian government attack effort.

Based on the DHS alert, the threat actors for this campaign employed a variety of tactics, techniques and procedures, including: spearphishing emails (from a compromised, legitimate account); wateringhole domains; credential gathering; opensource and network reconnaissance; hostbased exploitation; and targeting industrial control system (ICS) infrastructure. *Spear Phishing* are attacks targeting specific individuals, in this case by sending emails personalized to the recipient that are (or appear to be) from a legitimate account and usually entice the recipient to click on a link that injects malware onto their systems. Spear phishing emails currently are the most prevalent method for delivering advanced persistent threat (APT) attacks—84% of organizations have said a spear-phishing attack successfully penetrated their organization in 2015, with an average impact of $1.6 million per attack.[15] Those numbers have continued to increase.[16] *Watering Hole Domain Attacks* are where attackers discern websites a target group regularly uses (such as for trade organizations and information websites), and infect one or more of those websites with malware, usually aimed at collecting information and credentials of the user. Credential Gathering is a highly valuable attack because it enables attackers to use those credentials to gain access to the target systems and navigate within the system for recognizance and, potentially, to wreak havoc.

According to the DHS and FBI, the Russian attackers leveraged compromised credentials to access victims' networks *where multi-factor authentication was not used.* Multi-factor authentication is an important step for adding another layer of security by requiring more than one piece of evidence (such as a security key sent to a second device) to gain access to an account and, as the National Standards of Industry and Technology (NIST) advocates, should be used whenever possible.[17]

In addition to the March 2018 warning, in April 16, 2018, the DHS warned of a Russian government campaign to exploit infrastructure devices critical to utility operations in

---

[14] *DOJ press release, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged.*

[15] *FireEye, Spear-Phishing Attacks: Why They Are Successful and How to Stop Them, https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf.*

[16] *See, e.g., "Why 2017's Phishing Attacks Teach Us All to Beware," InfoSecurity Magazine, September 20, 2017, https://www.infosecurity-magazine.com/opinions/why-2017-phishing-attacks-teach/.*

[17] *https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication.*

the water and other sectors. DHS noted that the infrastructure network devices are often public facing and operating without sufficient security, thereby making them easy targets.[18] Factors increasing the vulnerability include:

- Insufficient antivirus, integrity-maintenance and other security tools, particularly for network devices used by small businesses and operating on residential-class routers;
- Manufacturers build and distribute the devices with exploitable services to make them easier to install, operate and maintain;
- Failure to change vendor default settings, enhance security and regularly patch systems and software;
- Failure to remove or update antiquated or outdated equipment that is no longer being supported by the manufacturer or vendor; and
- Overlooking network devices when assessing risk or recovering from a cyber intrusion.[19]

Foreseeability Mandates Due Diligence and Reasonable Efforts

Cybersecurity risks—whether in the form of technical mistakes, cyber-crime, espionage, "hacktivism", terrorism or warfare—continue to increase. One study reported that every sixty seconds cyber-crime costs more than $1.1 million and impacts more than 1,800 people.[20] Phishing attacks (22.9 per minute) and ransomware (victimizing 1.5 companies per minute) top the vulnerabilities list.[21] After the December 2015 attacks that shut down Ukraine's power grid, the U.S. government warned American power companies, water suppliers and transportation networks that the same methods of attack could be used against them.[22]

Technical and procedural security measures can help protect against many cyber threats. For example, phishing attacks can be reduced by teaching employees not to click on questionable links, and to have better filters that block or flag external, or suspicious, emails. The harm from ransomware attacks can be minimized with adequate system redundancies, tested backups and diligent updates and patches to block certain vulnerabilities. *Also, given that perhaps close to 90 percent of attacks are caused by human error or behavior,*[23] *it is essential to increase cybersecurity awareness, education, training and best practices within an organization.*

---

[18] *U.S. Department of Homeland Security (DHS), US-CERT, Alert (TA18-074A), Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, March 15, 2018, revised, March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A;*

[19] *Id. See also AWWA Utility Advisory, April 19, 2018 (summarizing the technical alert). http://social.bluehornet.com/hostedemail/email.htm?CID=38807374598&ch=B16C42F0EC4155D2BC94F867B6B1EC9D&h=6aeaa7c9c5c035bd55305248f17efb17&ei=Tso1WTu1N&schema=echo4.*

[20] *RiskIQ Evil Internet Minute 2.0 (2018) report, available at https://www.riskiq.com/infographic/evil-internet-minute-2018/ (also discussed at, e.g., https://www.pcmag.com/news/363217/more-than-1-1m-lost-to-cybercrime-every-minute).*

[21] *Id.*

[22] *David Sanger, "Utilities Cautioned About Potential for a Cyberattack After Ukraine's," New York Times, Feb. 29, 2016, available at https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html.*

[23] *Ross Kelly, "Almost 90% of Cyber Attacks are Caused by Human Error or Behavior, Chief Executive, March 3, 2017, available at https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/.*

While the legal determination of whether a particular incident was "foreseeable" might be disputed on a case-by-case basis[24], it is well established that public and private entities that fail to anticipate and prepare for a diverse set of cyber threats face a very real threat of civil and regulatory liability when incidents do happen. Courts and regulators—as well as the public, impacting reputational harm—are increasingly demanding that entities employ due diligence and reasonable measures to prevent, detect and respond to cyber risk. Cyber attacks have filled news headlines, there have been numerous warnings for critical infrastructure generally and the water sector in particular, and it is necessary to expect that your organization will be targeted. (It is now over-used but no less true: for cyberattacks, "it is not a question of *if* but *when*," and the answer may be the hackers already are in your systems and you do not know it.)

There are numerous examples of organizations facing multi-million dollar penalties for failing to employ reasonable measures to prevent, detect and respond to cyber threats. In one class action lawsuit, against an employer following a phishing scheme that compromised sensitive W-2 data of employees and their families, a federal district court in California stated: *[I]t is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently. Castillo v. Seagate Tech., LLC,* No. 16 Civ. 1958, 2016 WL 9280242, at *9 (N.D. Cal. Sept. 14, 2016). The employer subsequently paid $5.75 million to settle that lawsuit.[25] In a similar case, a New York federal court recently quoted *Castillo* and added: *Employers have a duty to take reasonable precautions to protect the PII that they require from employees. Sackin, et al. v. TransPerfect Global Inc.,* Case No. 1:17-cv-1469-LGS (S.D.N.Y.).[26] Also, in *FTC v. Wyndham Worldwide Corp.,* the U.S. Court of Appeals for the Third Circuit found that unreasonable data security would constitute "unfair and deceptive practices" under Article 5 of the FTC Act, 15 U.S.C., §45(a), and recognized that the Federal Trade Commission had authority to bring a civil regulatory action. 799 F.3d 236 (3d Cir. 2015). The Third Circuit found that Wyndham had "fair notice" of its potential liability for failing to employ "reasonable" data security measures. *Id.*

Thus, even if you are not certain exactly when or how your organization will suffer a cyber attack, it is critical to accept the reality that some type of cyber risk is at least foreseeable, perhaps inevitable. The reality and prevalence of cyber risk mandates that organizations and their leaders not only take meaningful action to prevent and detect harms, but also have a tested plan for responding swiftly and effectively when cyber incidents do occur. Failing to address cybersecurity risk in a proactive way can have devastating results.

Failing to take reasonable measures and employ best practices to prevent, detect, and swiftly respond to cyber-attacks means that organizations and the people who run them will face greater damage—including technical, operational, financial and reputational harm—when the cyber-attacks do occur.

---

[24] *For a legal discussion regarding the sometimes-elusive concept of "foreseeability" in civil tort (including negligence) actions, see, e.g., David Owen, Figuring Foreseeability, 44 Wake Forest L. Rev. 1277 (2009), available at https://scholarcommons.sc.edu/cgi/viewcontent.cgi?article=1937&context=law_facpub.*

[25] *Castillo, Order Granting Mot. For Final Approval of Class Action Settlement, etc., Docket No. 85 (March 14, 2018), available at https://secure.dahladmin.com/SEAGAT/content/documents/OrderGrantingFinalApprovalofSettlement.pdf.*

[26] *Available at https://www.leagle.com/decision/infdco20171005i57.*

Beyond Technical Risk: Reputational, Regulatory and Civil Liability Costs

In addition to technical damage and outages from a breach, an entity that fails to adequately protect its systems, operations, and customer data also faces the risk of reputational harm, as well as regulatory enforcement, criminal penalties and civil liability costs. Proposed legislation has even been introduced to impose criminal penalties for failing to timely disclose data breaches. The Data Security and Breach Notification Act, proposed in November 2017, sought to impose jail time for executives who actively conceal data breaches.[27] (That law was proposed on the heels of the Uber data breach disclosure, which involved the theft of data on 57 million customers; Uber paid the hackers $100,000 to destroy the stolen data, classified it as a "bug bounty payment,"[28] and failed to report the breach to regulators or the public for more than a year.)

Corporate executives and government officials have been called to testify before congress, been criticized in the media, and have lost their jobs as a result of how they prepared, or failed to prepare, for and respond to cybersecurity incidents.[29] The reputational damage to entities and individuals, and the cost of recovering from a poorly handled cyber incident response are significant and long lasting.

A robust approach to cybersecurity will help prevent cyber incidents, enable a far better response to incidents that do happen, and provide a far better explanation of preparedness and response when confronted by customers, constituents, investors, boards, regulators, civil litigants, legislators, and the media.

Examples of corporate executives and government officials who have lost their jobs as a result of cybersecurity breaches include, among others, the:

- General Counsel at Yahoo, after a state-sponsored hack and delayed disclosures;
- Director General of the Swedish Transport Agency and also the Minister of the Interior who lost his place in the Swedish Cabinet, after unauthorized access to the vehicle registration and drivers license database by third-party contractor IBM;
- CEO and CFO of Austrian aerospace company FACC, after a business email compromise (though this was not confirmed as the sole cause of termination);
- CEO of Sony Pictures, after a nation-state hack exposed corporate emails;
- CSO and also the Legal Director of Security and Enforcement of Uber, after paying $100,000 to hackers and failing to disclose a major data breach for more than a year;
- CEO, CSO and also the CIO of Equifax, after a major breach impacting more than 143 million Americans;

---

[27] *See Larson, Sandra, "Senators Introduce Data Breach Disclosure Bill," CNN Tech, Dec. 1, 2017, available at https://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html.*

[28] *Bug bounty programs, a way to crowdsource vulnerability testing, offer recognition and compensation to security researchers who report vulnerabilities and exploits to the organization so the problems can be fixed before becoming known to the general public. Many public and private sector organizations use bug bounty programs, including the U.S. Department of Defense, Pentagon, Google, Microsoft, Facebook, United Airlines and others. An increasing number of state governments also are considering adopting bug bounty programs. Bergal, Jenni, "White-Hat Hackers to the Rescue, Government Technology, May 14, 2018, available at http://www.govtech.com/security/White-Hat-Hackers-to-the-Rescue.html.*

[29] *https://www.csoonline.com/article/3158825/it-jobs/how-to-get-fired-in-2017-have-a-security-breach.html.*

- CEO and certain board members of Target, after a major retail breach that occurred when Target's third-party heating and air conditioning vendor was compromised.29F30

Also, the Federal Trade Commission (FTC) has brought more than 60 cases against companies for failing to have "reasonable" or "industry standard" cybersecurity practices, defenses and responses.30F31 The Securities and Exchange Commission, Department of Health and Human Services, banking regulators, and many states have also imposed fines and brought lawsuits against entities that failed to protect consumer data. In addition, private civil litigants and states attorneys general have obtained millions of dollars in settlements and penalties related to cybersecurity breaches.31F32

Government Actors: Sovereign Immunity May Not Protect You

Although principles of sovereign immunity may prevent, or at least hinder, civil actions against government actors, many government entities have nonetheless paid millions in settlements related to cybersecurity breaches. Sovereign immunity, a legal concept that protects federal and state governments from liability in many situations, also has exceptions as determined by statute. **Moreover, defending these lawsuits, and addressing the numerous other harms and costs that result from mishandled cybersecurity incidents (impacts on systems, data, operations, reputations and perhaps even personal safety) can be far more costly, distracting and damaging than taking a proactive approach to cybersecurity.**

If property damage, injury or death occur due to negligence or a wrongful act, claims may be allowed pursuant to the Federal Tort Claims Act (FTCA),[33] and comparable state laws that specifically waive immunity under those circumstances.[34]

Also, the Administrative Procedure Act (APA) governs internal procedures of administrative agencies, including how they interact with the public, and provides that final agency decisions are subject to judicial review.[35] The APA includes the federal Privacy Act (FPA), which governs how U.S. federal government agencies collect, maintain, use and disseminate personally identifiable information about individuals. The FPA includes a waiver of immunity where there is a (1) willful, intentional and improper disclosure of personal information that results in (2) actual harm.[36] As with the FTCA, many states also have comparable statutes to the APA and FPA.[37] (As discussed below, plaintiffs suing the Office of Personnel Management (OPM) for that massive data breach relied upon the APA and FPA.)

Examples where government entities have paid millions in settlements related to cybersecurity breaches impacting personal information include:

---

[30] *https://www.csoonline.com/article/2859485/data-breach/the-buck-stops-here-8-security-breaches-that-got-someone-fired.html#slide1.*

[31] *https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (page 4-5).*

[32] *https://www.f5.com/labs/articles/cisotociso/breach-costs-are-rising-with-the-prevalence-of-lawsuits.*

[33] *Title 28, United States Code, Sections 1346(b), 2671-2680.*

[34] *https://www.mwl-law.com/wp-content/uploads/2013/03/MUNICIPAL-COUNTY-LOCAL-GOVERNMENTAL-LIABILITY-CHART-00212510.pdf.*

[35] *Title 5, United States Code, Sections 551-559.*

[36] *Title 5, United States Code, Section 552a.*

[37] *See, e.g., http://www.uniformlaws.org/ActSummary.aspx?title=State%20Administrative%20Procedure%20Act,%20Revised%20Model.*

- Mille Lacs County in Minnesota paid $1 million to settle a class-action lawsuit after an employee allegedly accessed driver's license records of 379 residents without authorization.[38] The county fired the employee and, as required, notified the impacted individuals. In the lawsuit, plaintiffs alleged that the county had insufficient policies and "failed to put into place systems and/or procedures to ensure … class members' private data would be protected and would not be subject to misuse."
- Three years earlier, Rock County, Minnesota, paid $2 million for a breach where a county employee improperly searched the same database.[39]
- Maricopa County Community College in Arizona paid $26 million to settle a lawsuit and pay fees and costs to address a breach where hackers compromised multiple databases and stole personal information of two million employees, students and prospective students.
- Skagit County, Washington, paid $215,000 in fines imposed by the U.S. Department of Health and Human Services (HHS) for inadvertently uploading protected health information of more than 1500 people to a county public server. As part of the settlement, the county was required to draft written protocols, implement new policies and train all employees, as well as follow new reporting requirements. HHS said this case was a call to all local governments "to adopt a meaningful compliance program to ensure the privacy and security of Patients' information."

Where an entity hosts its own services and software it more likely would be held responsible for a compromise than if it contracts the hosting to a reputable third party or using cloud-based services. The breach of Superion's *Click2Gov* system potentially exposed tens of thousands of customers of local government, including many utility customers, in a number of states including California, Florida, Texas, Arizona and Wisconsin.[40] The *Click2Gov* system is used by hundreds of local governments for payment processing as well as other services, such as permit applications. Hackers apparently placed a digital card skimmer on top of Click2Gov code, compromising networks in certain towns and cities that locally hosted the software; notably, Superion's data centers and cloud-based services were not compromised. This creates questions of liability based on the governments' failure to implement proper security upgrades and monitoring, and whether Superion should have played a more proactive role.

Some lawsuits have been dismissed where a court finds plaintiffs have not shown the necessary level of harm from a breach or, where applicable, plaintiffs have failed to overcome sovereign immunity defenses. A federal district court judge in September 2017 dismissed the civil lawsuits brought, based on laws including the APA and FPA, against the Office of Personnel Management (OPM) for the breaches, disclosed in 2015 and attributed to a Chinese intelligence operation, which exposed highly sensitive security clearance information of more than 20 million people.[41] The court stated that there was insufficient evidence the individuals were actually harmed by the breach that exposed, among other information, details regarding finances, romantic relationships, substance abuse and some current, former and prospective government employees' fingerprints.

OPM officials had failed to encrypt highly sensitive data, did not fix known flaws in its systems and disregarded warnings from the OPM Inspector General that certain

[38] *http://www.governing.com/gov-institute/voices/col-cybersecurity-data-breach-government-liability.html.*

[39] *Id.*

[40] *http://www.govtech.com/security/Thousands-Exposed-in-Municipal-Website-Breaches.html*

[41] *In re: U.S. Office of Personnel Management Data Security Breach Litig., Misc. Action No. 15-1394, MDL Docket No. 2664, Mem. Op. dated Sept. 19, 2017, avail. at https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2015mc1394-117.*

systems failed to meet cybersecurity standards. The court, however, also noted the plaintiffs had failed to establish that OPM was not protected by sovereign immunity.[42] Plaintiffs have appealed that decision, meaning litigation costs continue to increase, as the law regarding liability for cyber breaches continues to develop.

CHALLENGES TO MANAGING CYBER RISK

For many utilities and other public infrastructure entities, the resources and capabilities for preventing, detecting and mitigating cyber risk fall short, particularly given the significance of the threat and potential harm. Challenges to managing cyber risk in the water sector are organizational, physical and technological. The water sector presents diverse challenges due to its varying drinking water and wastewater infrastructure, and the fact it is comprised of entities of vastly different sizes, capabilities, resources and types of ownership. Multiple governing authorities, on a federal and state level, oversee water and wastewater concerns regarding public health, environmental protection and security, among others.[43] Fractured organizational structure, often embedded within a multifaceted municipality, shared infrastructure with different levels of risk, and a prevalence of legacy—sometimes antiquated—systems increase the challenges of managing cyber risk. Some of these challenges are not unique to the water sector; according to the Brookings Institute, the vast majority of public agencies lack a clear cybersecurity plan.[44]

Large organizations often say it is hard to defend against cyber attacks due to their size and multi-faceted systems, underscored by the concern that one point of compromise across a global network with thousands of employees could cause harm. Smaller organizations often claim inadequate financial and personnel resources, and lack of the time and knowledge, needed to address cybersecurity issues. In either case, where to start and how best to prioritize cybersecurity defenses are challenging. Regardless of the size of the entity, executives, managers and boards are haunted by (or at least should be asking) key questions, including:

- Have we identified and adequately secured our critical data and systems?
- Are we doing enough to anticipate threats and prevent, detect and quickly respond to cyber attacks?
- Have we done a recent risk assessment and developed a plan to address known risks?
- Are we ensuring patches are up to date and employing encryption and access limitations?
- Are we addressing vulnerabilities caused by legacy, or outdated systems, and working with vendors to develop a priority-based plan, timeline and budget for adopting cybersecurity upgrades (and, if necessary, overhauls) to improve cybersecurity?
- Will we have a good explanation to give our clients, constituents, customers, regulators and shareholders when attacks do happen?

Water sector utility owners and operators tend to be advanced in emergency response and resilience planning based on their preparations for natural disasters; similar

[42] *https://www.mwl-law.com/wp-content/uploads/2013/03/MUNICIPAL-COUNTY-LOCAL-GOVERNMENTAL-LIABILITY-CHART-00212510.pdf.*

[43] *DHS and EPA Water and Wastewater Systems Sector-Specific Plan, 2015, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.*

[44] *https://www.brookings.edu/blog/techtank/2015/02/03/the-vast-majority-of-the-government-lacks-clear-cybersecurity-plans/.*

redundancy and recovery methods and structures to ensure continuity of operations and protect public health and the environment also must be applied in the cybersecurity context.[45] Although replacing legacy systems and networks can be extremely costly, it is essential to work with vendors and cybersecurity experts to implement updates and, if necessary, overhauls of outdated systems. Invoke the help of internal or external advisors to prioritize risk and develop a realistic approach and plan for enhancing cybersecurity. At a minimum, comply with basic standards including restricted physical and technical access, firewalls, logging and encryption.

When it comes to cybersecurity, how much is enough? How much is needed to spend on cybersecurity defenses and personnel? How much time, effort and resources should be focused on cybersecurity governance? How much is sensible to insure against cyber risk and to adequately protect systems, data and assets? How much regulation is helpful to increase smart cybersecurity, without unduly diverting resources to check-the-box compliance efforts, or quelling innovation and new technologies? These are not easy questions to answer, so that leads to another question: Is there a way to make this all easier, or at least less overwhelming for organizations of varying sizes?

STANDARDS, GUIDANCE, REGULATION AND INSURANCE

Standards, guidance, regulation and insurance are available to help water sector entities address cybersecurity issues and develop comprehensive cybersecurity policies, programs and procedures.

Standards, Guidance and Regulation

Standards, toolkits and regulatory mandates help guide water sector entities regarding cybersecurity defenses and requirements addressing technological, physical and personal considerations. A discussion of the water sector's regulatory authorities and critical infrastructure partners is provided in the DHS and U.S. Environmental Protection Agency (USEPA) Water and Wastewater Systems Sector-Specific Plan (SSP), including a list of authorities in Appendix 2 and list of Critical Infrastructure Partners in Appendix 3 of the SSP.[46]

For more specific guidance in building and enhancing a cybersecurity program and plan, resources developed by the National Institute of Standards and Technology and the American Water Works Association (AWWA) are particularly helpful.

NIST Framework & Publications

A key and especially helpful cybersecurity resource is the National Institute of Standards and Technology (NIST) framework. This is a voluntary set of standards, guidelines and best practices to manage cybersecurity related risk.[47] As NIST states, the "Cybersecurity Framework's prioritized, flexible and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security."[48] On April 16, 2018, NIST published a newer Version 1.1 of the Framework, which is fully compatible with Version 1; it includes additional

[45] *See DHS and EPA Water and Wastewater Systems Sector-Specific Plan, 2015, https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.*

[46] *https://www.dhs.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf. Also, the Water Sector ISAC published a "Roadmap to a Secure and Resilient Water and Wastewater Sector," May 2017, which address cyber risk management, https://www.waterisac.org/sites/default/files/public/2017_CIPAC_Water_Sector_Roadmap_FINAL_051217.pdf.*

[47] *https://www.nist.gov/cyberframework.*

[48] *Id.*

guidance on identity management and supply chain cybersecurity.[49] NIST also provides additional guidance, including through special publications (SPs) and webinars, including SP800, on computer security, SP1800 on cybersecurity practice guides, and SP500 on computer systems technology.

AWWA Guidance & Use-Case Tool

The AWWA provides *Process Control System Security Guidance for the Water Sector* and a supporting Use-Case Tool that also is very helpful for establishing and improving cybersecurity systems specific to operations technology (OT) but can also inform enterprise security practices. The Water Sector Coordinating Council, the USEPA and NIST have recognized the AWWA Guidance and Use-Tool as the foundation of a voluntary, sector-specific approach to implementing the NIST Cybersecurity Framework.[50] The *Process Control System Security Guidance for the Water Sector* identifies 12 cybersecurity "practice categories," and recommends specific, critical practices under each category that direct map water-specific application to the NIST Cybersecurity Framework.

In an effort to provide water utilities with actionable tasks, the Use-Case Tool generates a prioritized list of recommended controls based on specific characteristics of the utility. The user selects from a series of pre-defined use cases that represents the type of functions their process control system may perform. The Use-Case Tool places emphasis on actionable recommendations with the highest priority assigned to those that will have the most impact in the short term. It should be noted, that the tool does not assess the extent to which a utility has implemented any of the recommended controls.

HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA), while specific to "covered entities" and "business associates" providing medical services or handling personal health information, provides a HIPAA Security Rule that can provide helpful cybersecurity guidance event to non-HIPAA regulated entities.[51] Regardless of whether your organization must comply with HIPAA, the HIPAA Security Rule "provides a clear, jargon-free framework for developing information security policies and programs" and can help municipalities and other water sector owners and operators build a solid foundation for cybersecurity programs.[52] In particular, as Jeffrey Morgan notes in a *CIO.com* article,[53] the final six pages of the HIPAA Security Rule, includes a helpful matrix on required actions for administrative, physical and technical cybersecurity safeguards.

State and Federal Regulation

Certain states have enacted regulations or provided guidance to address and prioritize cybersecurity in the water sector. For example, on July 21, 2017, New Jersey enacted the Water Quality Accountability Act (WQAA, effective as of October 19, 2017), which established new requirements designed to improve the safety, reliability and administrative oversight of the water infrastructure.[54] The Act applies to public water

---

[49] *Id.*

[50] *https://www.awwa.org/cybersecurity.*

[51] *HIPAA Security Rule, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.*

[52] *Morgan, Jeffrey, CIO.com, County and Municipal Cybersecurity, Part 2, April 3, 2017, https://www.cio.com/article/3186510/government-use-of-it/county-and-municipal-cybersecurity-part-2.html.*

[53] *See HIPAA Security Rule, cited above; see also, Morgan, Jeffrey, CIO.com, HIPAA as an Umbrella for County/Municipal Cybersecurity, https://www.cio.com/article/3188667/governance/hipaa-as-an-umbrella-for-countymunicipal-cybersecurity.html.*

[54] *New Jersey Statutes Annotated, 58:31-1, et seq., available at http://www.njleg.state.nj.us/2016/Bills/PL17/133_.PDF.*

systems with more than 500 service connections—approximately 300 water systems in New Jersey.[55] The New Jersey WQAA requires covered water system operators to inspect, maintain, repair and update their infrastructure consisting with AWWA standards, and requires water system operators with internet connected control systems to create cybersecurity programs and join the NJ Cybersecurity and Communications Integration Cell, designed to foster better collaboration and improved cybersecurity defenses.[56]

New York Public Health Law requires water suppliers to develop and submit emergency plans that, among other things, include "a vulnerability analysis assessment, including an analysis of vulnerability to terrorist attack and cyber attack, which shall be made after consultation with local and state law enforcement agencies."[57]

Connecticut's Public Utilities Regulatory Authority (PURA) set forth a Public Utilities Cybersecurity Action Plan with Compliance Standards and Oversight Procedures, dated April 6, 2016.[58] The Connecticut Plan seeks to increase partnership among utilities, increase monitoring and develop an enhanced "culture of security" to address cyber risk. The Connecticut Plan references the AWWA Guidance and Use-Tool and the NIST Framework, among other guidance for improving cybersecurity.[59]

At the federal level, the recent America's Water Infrastructure Act of 2018,[60] requires community water systems serving a population of more than 3,300 persons to conduct a risk and resilience assessment of their systems (42 U.S.C. 300i-2). This includes assessing the security of any electronic, computer, or other automated systems that the community water system uses. The Act also requires covered community water systems to certify to the USEPA, starting in March 2020 and re-certifying every five years, that they have completed the required assessments.

Cyber Insurance

Cyber insurance is an important consideration for both private-sector and government entities and also provide guidance regarding an organization's cyber risk profile. Determining the proper type and amount of cyber insurance requires a rigorous assessment of risk, and evaluation of specific coverage and policies. It is important to understand what data and systems are covered, to what extent, and for what incidents and responses. Coverage often varies among insurers, and from policy to policy. The scope of cyber insurance is an emerging area based on currently limited data analytics. Therefore, it is important not only to ask whether an entity has "cyber insurance" but to work with a knowledgeable advisor regarding specifically what is and may not be covered under the entity's policies.

The issue of cyber insurance can be difficult for most entities, and is often more complex for state operations, due to the sprawling nature and diverse systems that exist

---

[55] *http://www.nj.gov/dep/watersupply/g_reg-wqaa.html.*

[56] *Id.*

[57] *New York Consolidated Laws, Public Health, Article 11: Water Supply Emergency Plans, Section 1125, https://www.nysenate.gov/legislation/laws/PBH/1125.*

[58] *http://www.ct.gov/pura/lib/pura/electric/cyber_report_April_6_2016.pdf; see also Connecticut Office of Legislative Research report November 2, 2016, https://www.cga.ct.gov/2016/rpt/pdf/2016-R-0274.pdf.*

[59] *http://www.ct.gov/pura/lib/pura/electric/cyber_report_April_6_2016.pdf.*

[60] *Congress passed the bipartisan Act in October 2018 and, at the time of publication, it was pending signature by the President. https://www.congress.gov/bill/115th-congress/senate-bill/3021/text?q=%7B%22search%22%3A%5B%22s+3021%22%5D%7D&r=1*

for many states.[61] According to the 2017 State CIO Survey, 38 percent of state CIOs reported having some type of cyber insurance, up from 20 percent in 2015.[62] Thus, for a government utility, it may be advisable to have a utility-specific cyber policy, in addition to whatever policy may apply more broadly to the government, or at least to ensure that existing policies address the utility's potential cyber risks.

PRIORITIZING CYBERSECURITY SOLUTIONS

Key to a good cybersecurity plan is understanding the threat and establishing cybersecurity governance protocols for addressing and managing the risk across the enterprise. To do this effectively requires executive support. Senior leadership—including the Board, Chief Executive Officer, Governor's Office, Municipal Executive—needs to be invested in ensuring cybersecurity is taken seriously in the organization. Also, because the issues and solutions are multi-faceted, an interdisciplinary team is required, examining the concerns from a technological, cost, efficiency, personnel and legal perspective.

Start by asking some basic questions:

- **WHAT** do we need to protect and **WHY**?
  - This requires understanding and then assessing risks within the organization in terms of technology, physical security and personnel. Senior leadership and technical experts within the organization need to confer, with the help of outside advisors if necessary. Do not overlook the fact that almost 90% of cyber attacks are caused by human error or behavior and those risks must be managed by limited access to systems and data to those critical for business functions.[63] Also, third-party vendors, partners and service providers who may have access to your systems and data also provide vulnerabilities that must be considered and managed.[64]
- **WHO** is the lead for cybersecurity within the organization?
  - The cybersecurity team should be interdisciplinary and the lead for the organization should have a direct line to senior management; as has been said many times, cybersecurity—particularly in terms of critical infrastructure—is not just a "tech" issue but also a critical component of enterprise risk management.
- **HOW** are we going to allocate resources, evaluate options and prioritize solutions?
  - Based on the risk assessment, develop a cybersecurity plan and protocols. NIST and the AWWA Guidance and Use-Tool are particularly helpful for prioritizing areas, analyzing gaps and developing a plan, including for cost-effective solutions such as two-factor authentication, restricted access, regular patches and updates, and education that fosters a culture of security and awareness throughout the enterprise.

---

[61] *Bergal, Jenni, "Worried About Hackers, States Turn to Cyber Insurance," Insurance Journal, Nov. 13, 2017, available at https://www.insurancejournal.com/news/national/2017/11/13/470991.htm.*

[62] *https://www.nascio.org/Portals/0/Publications/Documents/2017/NASCIO_2017_State_CIO_Survey.pdf?ver=2017-10-25-174540-510.*

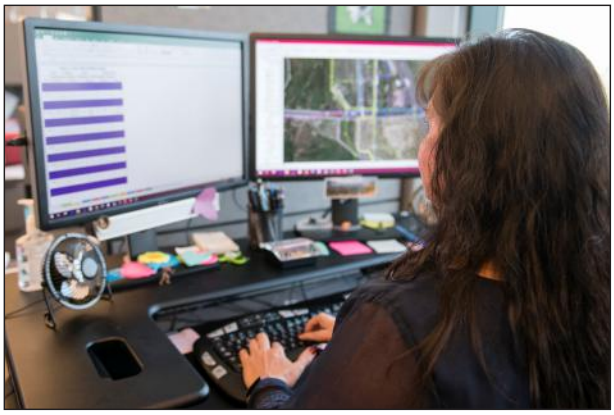
[63] *https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/.*

[64] *Germano, Judith, Third Party Cyber Risk and Corporate Responsibility, https://www.lawandsecurity.org/wp-content/uploads/2017/02/Germano.NYU_.ThirdPartyRiskWhitepaper.Feb2017.pdf.*

- Many, particularly smaller and mid-sized organizations or those with a less sophisticated cybersecurity posture and experience may find outsourcing—of governance and technical advisors as well as for cloud-based services and functions—can provide greater expertise and security than the organization may have or be able to provide internally.
- It also is critical to recognize that this is an organic and evolving process that requires regular assessments and continual updates to technology and processes to optimize cyber defenses.

In partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology ISAC, the WaterISAC has developed a list of 10 basic cybersecurity recommendations that water and wastewater utilities can use to reduce exploitable weaknesses and defend against avoidable data breaches and cyber attacks:[65]

1. Maintain an Accurate Inventory of Control System Devices and Eliminate Any Exposure of this Equipment to External Networks;
2. Implement Network Segmentation and Apply Firewalls;
3. Use Secure Remote Access Methods;
4. Establish Role-Based Access Controls and Implement System Logging;
5. Use Only Strong Passwords, Change Default Passwords, and Consider Other Access Controls;
6. Maintain Awareness of Vulnerabilities and Implement Necessary Patches and Updates;
7. Develop and Enforce Policies on Mobile Devices;
8. Implement an Employee Cybersecurity Training Program;
9. Involve Executives in Cybersecurity; and
10. Implement Measures for Detecting Compromises and Develop a Cybersecurity Incident Response Plan.



Partnerships, within the organization, within the sector, and among public and private entities are critically important for successful cybersecurity and cyber risk management.[66] Sharing threat information, solutions, best practices and other resources can provide greater security that benefits the sector as a whole. When it comes to cybersecurity in the water and wastewater sector, far more is to be gained by collaboration and communication than competition.

The cybersecurity landscape is changing rapidly as threats and technology continues to evolve. Given the severity of risk and potential harm, cybersecurity is a top threat that must be made a top priority for the water and wastewater sector. It is critically important to take a proactive and comprehensive approach to cybersecurity, involving active participation of the senior leaders of the organization, to ensure adequate technological and governance procedures are in place as part of an enterprise-wide cybersecurity program and strategy.

[65] *WaterISAC, Security Information Center, 10 Basic Cybersecurity Measures, Best Practices to Reduce Exploitable Weaknesses and Attacks, June 2015, https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf.*

[66] *Germano, Judith, Cybersecurity Partnerships, A New Era of Public-Private Collaboration, NYU School of Law, http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf.*

American Water Works Association