Cybersecurity: A Foundational Requirement for a Modern Water Utility

Contents

Executive summary

Water utilities are faced with many challenges, from aging infrastructure, an aging workforce, and climate change to the increased cost of operating and maintaining facilities and, in many instances, reduced revenue due to global crises.

Intelligent water and Internet of Things (IoT) solutions have been paving the way to help water agencies do more with less, increase efficiency, and provide better service to customers. However, as a result of adoption of new technologies, such as digital networks, real-time data acquisition and analytics, and remote operations, water systems are not as airtight as they used to be, and the door has been opened to substantial cyber risks for critical infrastructure. This has been the premise behind the 2018 America's Water Infrastructure Act (AWIA), which requires community water systems serving more than 3300 people to develop or update their risk assessments and emergency response plans, including Operational Technology (OT) cybersecurity.

This document provides a summary of best practices and key approaches for water utilities to identify cyber vulnerabilities and adopt solutions that result in a reliable and robust security foundation, so that they can ensure public health and operational resiliency. The following topics are discussed:

- The balancing act between operational risk and operational continuity
- A Risk Management Framework (RMF) that aligns risk, exposure with consequence, and treatment, and insight into CapEx and OpEx trade-offs
- The need to protect Industrial Control System (ICS) networks by having a clear and well-defined separation of the OT, enterprise network, and cloud infrastructure
- The reasons why people are a critical aspect of an effective cybersecurity adoption, and why having a security culture in the organization is a key attribute to success

Introduction

Water is a critical resource and is not only the key to the basic needs of life and health, but also an enabler of important industries such as agriculture, power generation, construction, technology, and nearly every other core domain that shapes civilization as we grow into the 21st century and beyond. The environmental stewardship of this priceless resource must be prioritized. A responsible and sustainable balance must be struck between water use and preserving the environment that thrives on and supplies the water.

As population centers shift, both local and global water supplies are increasingly strained. Unlike land or fossil fuels, which are geologically locked in place, water is not an isolated asset. It is constantly traveling the earth and moving in the form of rivers, streams, ocean currents, clouds, and slow-moving glaciers and icebergs. This necessitates water-sharing agreements across organizations and nations.

Addressing the water quality of a river that flows the length of a continent is no small challenge, and local water agencies must do their part to ensure proper extraction and treatment of the water, as well as the responsible discharge of wastewater back into the environment. In addition, secure operations are a key aspect of effective water stewardship, and a strong cybersecurity strategy is necessary to ensure the continued presence of clean water for consumers and the environment. As we move deeper into a world that is driven by technology, a clear trend of increasing cybersecurity threats is emerging. The consequences of a breach to a water organization can include production disruption, contamination, unintended discharge with negative environmental consequences, equipment failure, and interruption of service to the consumer. A breach can also result in additional costs and compromised personal information of consumers and employees.

Today water organizations face increasing stress on their infrastructure. Water shortages and rationing, the need to ensure water quality, changing weather patterns, and aging and leaking infrastructure are all real challenges. A new set of digital technologies with transformative potential is being introduced in the marketplace to address these present and imminent challenges. Many water utilities have started their digital transformation journey, unlocking new capabilities and increased business value and insight. This is an important step forward, but there are many potential security vulnerabilities that need to be addressed. As utilities cross into this new era, bringing the old systems alongside the new and integrating OT and IoT/modern technologies, it is important to address the cybersecurity dimensions of water networks. Gone are the days of reliance on air gaps and simple perimeter defense as being sufficient to address all outside threats. Water organizations must consider many threat vectors and build an architecture that recognizes the perimeter as everywhere, providing tools to address segmentation, access, anomalous behavior, application performance, identity, and trust.

United States cybersecurity regulations

Recent history

U.S. Homeland Security Presidential Directive 7 was superseded in 2013 by Presidential Policy Directive 21, which expanded the list of critical infrastructures from 7 to 21 and renamed the Water Sector to the Water and Wastewater Systems Sector. The U.S. Environmental Protection Agency (EPA) is the agency for the Water and Wastewater Systems Sector and works with the Department of Homeland Security (DHS), other agencies, and industry groups to improve security for water and wastewater systems. In response to Presidential Policy Directive 21, DHS issued the National Infrastructure Protection Plan, which provides an updated approach to critical infrastructure security.

Also in 2013, Presidential Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, established that:

“It is the Policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”

EO 13636 also called for development of a voluntary risk based cybersecurity framework, as set forth in industry standards and best practices, to help organizations manage cybersecurity risk. As a result of EO 13636, the National Institute of Standards and Technology (NIST) published the Framework for Improving Critical Infrastructure Cybersecurity, and the American Water Works Association (AWWA) published the Process Control System Security Guidance for the Water Sector. Additionally, NIST has revised a number of its SP 800 series standards in the years since EO 13636 was issued.

Presidential Policy Directive 21 and EO 13636 have led to an increased focus on national policy regarding ICS security in critical infrastructure. Industry associations and government agencies are making concerted efforts to quickly educate utilities. The guidelines and standards from these groups and agencies are designed to affect the way critical infrastructure projects are engineered and implemented. These guidelines apply to any entity, public or private, that runs critical infrastructure facilities.

The EPA’s response to EO 13636 recommends using a voluntary approach to foster compliance with the cybersecurity framework developed by NIST. However, the EPA closed its response with the following statement: “If the voluntary partnership model is not successful in achieving widespread implementation of the Cybersecurity Framework or if warranted by a changing cybersecurity risk profile, the EPA can revisit the option of using general statutory authority to regulate cybersecurity in the Water and Wastewater Systems sector.”

Current regulations

The AWIA was signed into law on October 23, 2018. The law requires community (drinking) water systems serving more than 3300 people to develop or update risk assessments and Emergency Response Plans (ERPs). The law specifies the components that the risk assessments and ERPs must address, and for the first time it includes cybersecurity. The law establishes deadlines by which water systems must certify to EPA and complete the risk assessment and ERP. Table 1 illustrates the certification deadlines for the risk assessment and ERPs based on population served. This law provides the imminent framework for ensuring cybersecurity for water utilities.

Table 1. AWIA certification deadlines

Population served	Risk assessment due	ERP due[1]
≥100,000	March 31, 2020	September 30, 2020
50,000 to 99,999	December 31, 2020	June 30, 2021
3,301 to 49,999	June 30, 2021	December 30, 2021

[1] ERP certifications are due six months from the date of the risk assessment certification. The dates shown here are certification dates based on a utility submitting a risk assessment on the final due date.

Correlating cyber risk to operations

Given today's substantial cyber risks to critical infrastructure and the current regulatory requirements, water utilities have realized the value of adopting and investing in robust and reliable cybersecurity platforms and solutions. In the past, the water industry was less vulnerable to cyber threats, as utilities had the ability to switch to manual plant operation while the ICS cybersecurity concerns were addressed. A lesson learned in times of extreme circumstances, such as those we are facing with the COVID-19 outbreak in 2020, is that one cannot take labor availability for granted. Decisions by local authorities and the concerns of individual citizens may affect utilities' ability to manually control facilities for prolonged periods of time, resulting in a swing toward plants and processes being operated remotely. This in turn increases the risk to water utilities, as it has been shown that threat actors intensify their activities during crises and specifically target critical infrastructure.

Sweeping trends, new technologies, and now the global pandemic are reshaping how water and wastewater treatment plants are operated, now and into the future. Utilities will require a more mature formulation of objectives for water security. Executives and boards charged with sponsoring adoption and investment in cybersecurity, and ultimately with endorsing management's proposed cybersecurity programs, rely on mature methods for cyber risk evaluation and cybersecurity program strategies designed to promote cyber resiliency within the industrial network. Key elements of a successful cybersecurity approach include effective next-generation endpoint protection, an effective demilitarized zone (DMZ), and the ability to monitor and control assets over a protected network.

The relationship between operational risk and operational continuity to produce, store, and deliver water is as important and sensitive as ever. Utility managers are faced with a balancing act between the seemingly endless number of malevolent threats targeting their networks, people, and processes and defining their security posture, while trying to address physical and cybersecurity concerns to secure control systems and maintain critical operations across the business.

Risk Management Framework (RMF)

Successful achievement of the targeted outcomes in water and cybersecurity is a result of a comprehensive Risk Management Framework (RMF), applied with buy-in from management and collaborative efforts between control systems engineers, engineering managers, cybersecurity teams, and asset strategy, planning, investment, and risk teams. This approach is yielding valuable insights into the CapEx and OpEx trade-offs involved in a resilient cybersecurity program, and it provides managers and business leaders with the confidence that the organization can adequately detect, repel, and survive a cyberattack.

Enlisting an RMF to align risk, exposure with consequence, and treatment gives providers of cybersecurity technologies and services a quantified approach that helps them break down this complex problem into simpler terms and speak to decision-makers in a language they comprehend: corporate impact.

Securing water networks from cyber threats

In the past, water utility networks have been proprietary and standalone systems by design, using specialized hardware and software that were typically deployed in an air-gapped silo, away from external threats. Therefore, ICS was not designed with cybersecurity as a concern. Communication protocols such as Modbus and Profinet supervise, control, and connect ICS devices, but they lack the ability to authenticate users or find abnormal behavior. Many of these systems operate with outdated hardware components and old software with known vulnerabilities. As today's ICS has become IT-centric and highly connected due to the introduction of secondary networks such as IoT, it is exposed to the same online threats that IT systems face, but without proper cybersecurity solutions.

As a rule, ICS must operate continuously and reliably. Disruptions or failures in these systems can result in death or injury, property damage, and loss of critical life support services. Upgrading or even patching machines while maintaining operational efficiency is by no means a trivial process and can result in organizations using outdated systems for years before upgrading. Many applications share a single software library, and updating that library could break critical processes, requiring any change in production to undergo robust testing and potentially a change in logic.

ICS faces serious threats from cyberterrorism, including nation states conducting ongoing sophisticated hacking campaigns against these legacy, unpatched systems that can impact the nation, the economy, and public health. Consequently, the federal government now has a heightened awareness concerning the state of cybersecurity for the nation's critical infrastructure.

In fact, in 2013 the SOBH Cyber Jihad hackers launched a cyberattack against the Bowman Dam in New York. One of the computers that controlled the infrastructure was connected directly to the internet, and a combination of poor network design and lack of visibility allowed the attacker to pivot into the ICS in the OT environment and obtain information on operations, including water levels, temperatures, and the status of machinery. The attacker had the ability to do damage, and ultimately flooded the city of Rye, New York. Luckily, no serious harm was caused in this case. List reference: http://www.nation-e.com/blog/new_page_759.

Protecting ICS networks

This brings us to the first rule of protecting the ICS networks, which is to minimize control system exposure. Having a clear and well-defined separation of the OT, enterprise network, and cloud enables organizations to employ well-defined border protections in each part of the network. Cybersecurity shares many similarities with physical security. Gates, walls, and fences typically line the perimeter of a facility and are used to keep people, animals, and vehicles from crossing into the property. However, just because a fence exists doesn't mean access is forbidden. Authorized users such as employees and delivery personnel will be allowed to enter the facilities, with inspection at the entrance. In the networking world, this action is performed by firewalls and an industrial DMZ (iDMZ).

The iDMZ is a network segment that sits between the IT and Industrial Automation Control System (IACS) networks to prevent devices outside the facility from directly accessing those within. Think of it as the waiting area while your documentation is being checked. The firewall is the gatekeeper. It checks who is sending the traffic, what location they are sending it from, and, with next-generation firewalls, what the traffic is implying and what files are contained in the payload.

The ancient city of Babylon had the first known DMZ (Figure 1). The city was divided into two parts: the marketplace, where all the trade happened, and the inner city, where the residents lived. The outer wall was built to protect access into the marketplace. It allowed guards to monitor the entranceway and gave people a safe place to trade. However, access through the first border did not guarantee entry to the inner city. Entry through the inner gates was controlled, making the marketplace the DMZ between the outer lands and the inner city. The ICS is the inner city, an important resource that must be protected.

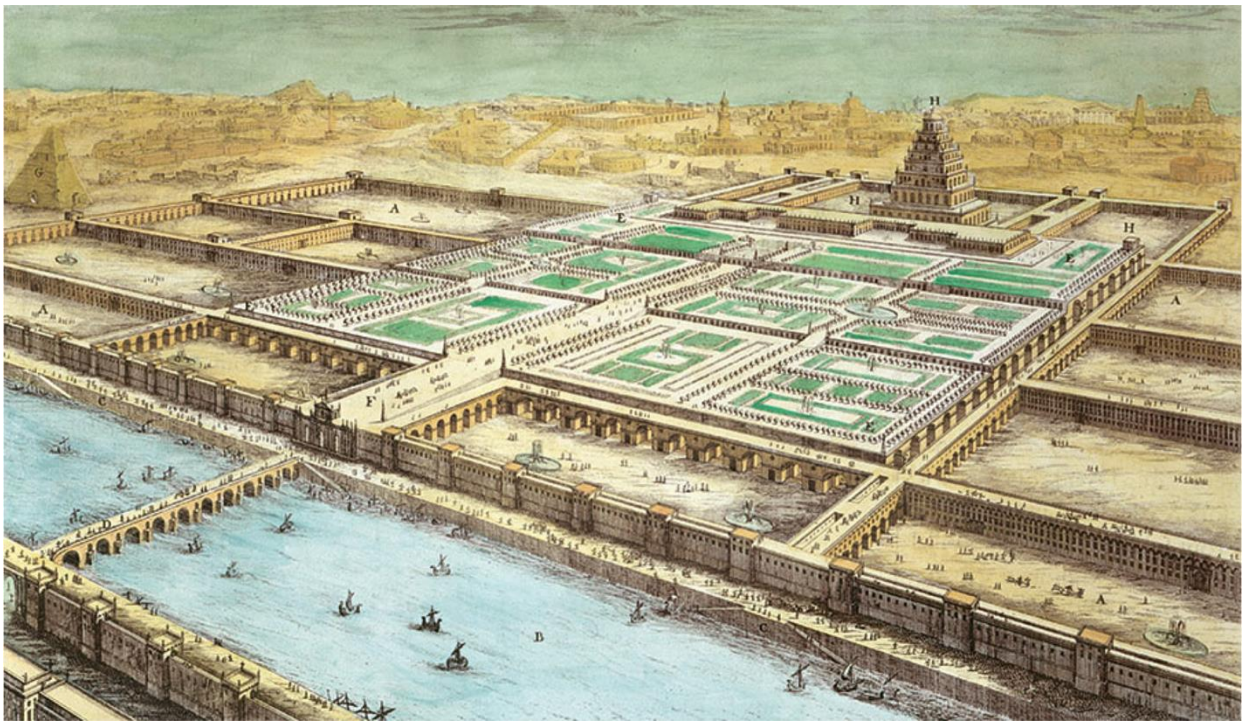

Figure 1.
DMZ of the ancient city of Babylon

We can take some comfort in the fact that critical assets are well protected from the most threatening source of malware. Next-generation firewalls are getting more and more sophisticated and intelligence feeds are getting more and more intelligent. However, simply protecting the boundary is not enough. Ransomware and malware can come from within. If an attacker does infiltrate the network, what systems are in place to stop it? Maroochy Shire is a small town in Queensland, Australia, that has an average of 10 million gallons per day of sewage flowing into its treatment center. Vitek Boden, an employee of the company that installed the sewage pump control system, resigned from his job after a dispute with his employers and was later rejected by the district council for a role as an inspector. His retaliation? To dump over 200,000 gallons of sewage into the rivers. Boden, as a former worker with access to system credentials, managed to hack into the network from a remote location and spoof his computer as part of the Supervisory Control And Data Acquisition (SCADA) network. List reference: https://medium.com/curious-minds/what-the-maroochy-incident-taught-us-about-cyber-warfare-4a1abd6abcfc.

Zero-trust networking was introduced to solve this type of problem. Zero trust means that just because one has access to the network does not mean that one inherits trust. In short, never trust, always verify. In 2020, NIST released a second draft of SP 800-27 for its zero-trust architecture, stating that cybersecurity is moving away from static perimeter control and shifting focus to users, assets, and resources. Although perimeter controls have their place, more emphasis is needed on protecting the assets within.

In Boden's case, if user verification had been in place, he would never have been able to access the sewage controls, and the damage would have been mitigated. Role-based access control (RBAC) in the physical world limits employee or visitor access to specific rooms and buildings depending on their job function or authority. Should the cleaners have access to the water quality testing facilities? Or, back to our example above, should ex-employees or contractors have access to the premises? Why treat the network any differently? When a user connects to the network, his or her identity must be verified, and only necessary resource access should be granted to that user. The engineers should not have access to the human resources database in the same way that the sales representative should not have access to the controls.

But how can we ensure that users are who they say they are? For an employee or a contractor, this is typically done with multifactor authentication (MFA). MFA ensures that access cannot be granted with stolen credentials. For example, suppose that a bad actor on the network gets access to the credentials of a SCADA systems administrator and logs in to the network as that user. From an ICS standpoint the individual would have high privilege and could inflict serious damage. If MFA has been adopted, that bad actor may also need access to the SCADA administrator's phone to respond to a push notification, which is locked behind a fingerprint or face scanner.

If network users can verify themselves with multiple actions, it is safe to assume they are legitimate. On the other hand, guests who visit the facility will not have network registrations but may be given access to guest Wi-Fi. These users can be assigned generic guest privileges, and the guest network should be physically air gapped from the remainder of the network.

With the surge of secondary or IoT networks in water utility environments, it's not just people who are on the network. In fact, water utilities probably have more "things" on the network than people. A robust security system begins with identifying critical assets, comprising the hardware/software and protocols deployed throughout the industrial network that facilitate automation and remote control of the treatment plants or pipeline systems. This means investing in systems that can passively interrogate networked assets in order to determine their make/model and firmware versions without the potential for a service disruption. One approach to passive interrogation is packet capture analysis, which avoids any active interrogation of the production assets' active service ports. This may take time, however, as passive network monitoring techniques will catch only traffic that passes through capable sensors. If done correctly, the addition of active probes can be a fast way of identifying assets, and can enable the discovery of endpoints that the switch never sees.

The creation of asset inventories is the first technique mentioned in WaterISAC's "15 Cybersecurity Fundamentals for Water and Wastewater Utilities," released in 2019. Such inventories allow for a detailed mapping of the interconnections between assets to better understand process dependencies correlated to active network protocols and can, in turn, enable the creation of network policies for traffic enforcement. Given the sensitivity of critical assets, functional clusters should be segmented into logical network zones. Due to the real-time nature of these systems, the use of partitioning controls within the zones themselves is not recommended; rather, it is important to control the communication among zones. This would ensure that if one zone becomes compromised or emits strange behavior due to user error, lateral movement would cease to affect other ICS resources.

NIST's cybersecurity framework, adopted by the AWWA, categorizes a core security framework into five steps: identify, protect, detect, respond, and recover. Thus far, this document has commented on the capability to identify and protect, but if we are already identifying, what do we need to detect? Detection refers to the constant monitoring of activities on the network. Pivoting back to the physical world, cameras are deployed across facilities for added security measures and have a record that can be reviewed when investigating an incident. Similarly, network monitoring tools provide visibility into all activities that happen in the network and keep a record for tracing anomalies and outliers.

There are specific tools in the marketplace that focus on operational protocols. It is critical to detect foreign protocols or assets that use protocols that they weren't designed to use (such as a guest device sending Modbus frames). In addition, it is highly important to have a monitoring tool that compares traffic against known vulnerability signatures for the devices in the utility, or against a known baseline of activity. This can give network administrators real-time alerts so that mitigation can begin before significant damage occurs.

Producing meaningful event and security notifications to permit operators to react immediately while eliminating false positives is the ultimate objective from a monitoring standpoint. Determining practical risk involving a production asset based on identified vulnerabilities, likelihood, consequence, competency, and level of effort is an effective means of tuning such a system.

As it is today, no single product, technology, or methodology can fully secure water networks. Protecting ICS assets requires a holistic defense-in-depth security approach that addresses internal and external security threats. Consider a medieval castle as an example (Figure 2). The first line of defense was always a deep moat that surrounded the perimeter, giving enemies only a single entrance to penetrate. If the moat was crossed, the enemy would then have a large stone wall to break through. But the fortifications didn't end there. There were always precautions in case both the first and second lines of defense were broken, making attackers face obstacle after obstacle before reaching the king in his keep. Effective cybersecurity follows the same fundamentals. Attackers may be able to breach one or maybe even two lines of defense, but it becomes exponentially more difficult with each additional line.

Controlling access and environment and maintaining a common battlefield picture have been key concepts for ancient and modern warfare. This is a critical security concept, one that has saved lives and facilities over time.

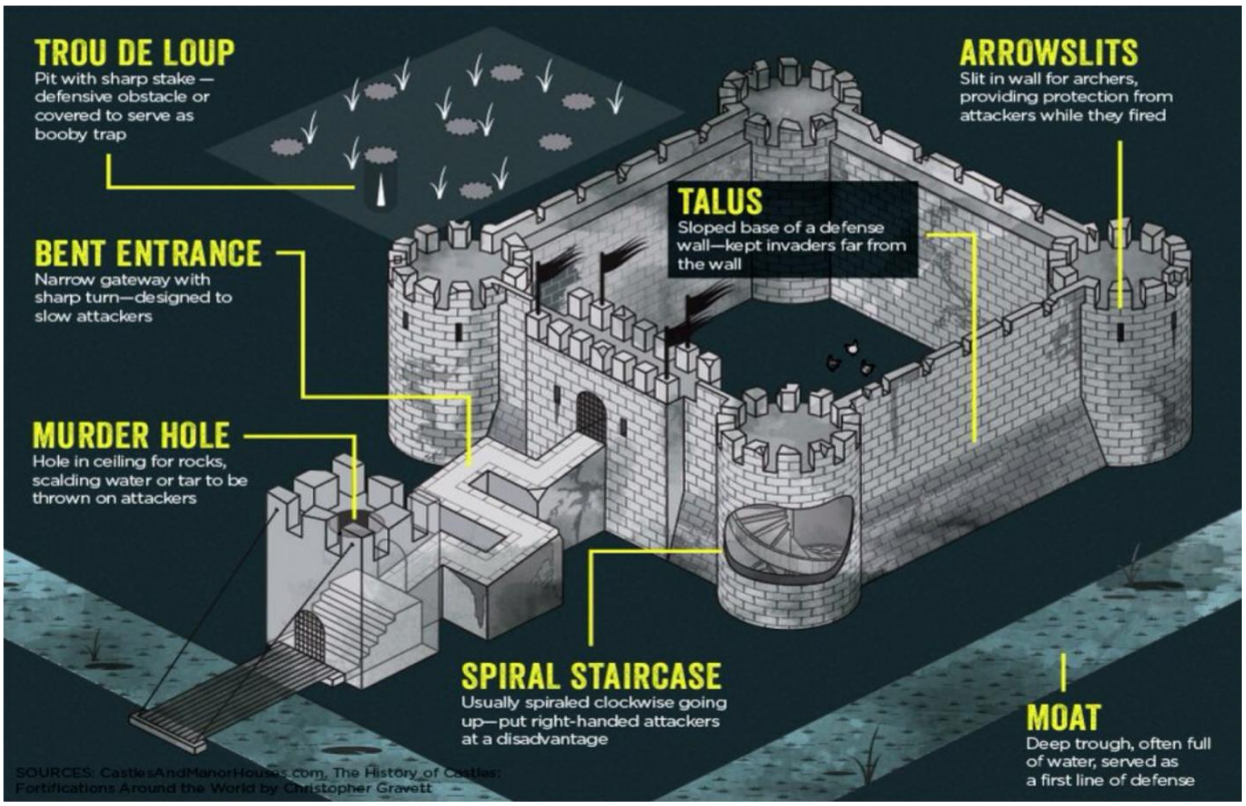

Figure 2.
Defense in depth

People's role in cybersecurity

People are just as critical to the process of ensuring cybersecurity for water facilities as the technology that has been deployed. Having a security culture in the organization is the glue that brings all these concepts together. NIST recommends that all personnel receive regular, ongoing cybersecurity awareness training. Role-specific training should be given to staff, including executives, operations engineers, SCADA engineers, and network administrators. For their people to be effective, water utilities need to establish cyber and operational resiliency strategies developed within the organization's policies and procedures. This will ensure a standardized approach to problem-solving, continuity of operations, and emergency response planning. Employing organizational standards, employees will be able to follow a predefined and rehearsed process without reliance on individual practices.

Cisco's John Chambers famously said, "There are two types of companies: ones that have been breached and those that do not realize it." To round out the NIST cybersecurity framework, a threat defense that helps the organization react to and minimize the impact of an attack that has occurred is critical. Organizations must be able to back up and restore their systems regardless of whether an event was caused by a cyberattack, human error, or physical failure. Unfortunately, many organizations do not find out that they lack proper backup and recovery plans until after an event has occurred. This reduces the speed of recovery and is often more expensive to repair. A planned and tested recovery strategy, along with a strong communication plan, are keys to reducing the impacts of a cyberattack.

Conclusion

Water organizations will face increasing pressures from both historical challenges that continue to intensify and new pressures from a rapidly evolving world. Digital transformation of water utilities provides the opportunity to combat many of these challenges by giving them much better visibility into assets and operations of critical facilities, capability for remote operations, and increased efficiency. While the transition may take some effort, today's intelligent water solutions have the ability to transform the business, leveraging new systems and technologies that were not available in the past. As a result operations will improve without compromising security. A robust cybersecurity foundation is the key element that will protect critical water and wastewater assets as utilities embark on their modernization journey.

It is thus imperative for water utilities to perform a thorough assessment of their systems and assets and understand their vulnerabilities, followed by devising a robust plan for ensuring cybersecurity throughout their digital implementation efforts. Planning today for the secure infrastructure of tomorrow should be a top priority in this transformative time. As the water industry embraces technological innovation, the benefits to the organizations, the consumers, and the environment will be embraced in a secure, reliable approach that assures access to this valuable resource well into the future.

For more information

Websites

Cisco: cisco.com/go/smartwater

Jacobs: jacobs.com/capabilities

Authors' biographies

Sielen Namdar, PE, Industry Executive, Global Water Business Lead, Cisco

Sielen is an industry executive with Cisco's Cities and Communities team and leads Cisco's Global Smart Water Business. She also serves as the co-chair of America's Partnership Group for Smart Water Networks Forum (SWAN). Sielen and her teams help water and wastewater customers globally build more resilient systems and operate, maintain, and manage their facilities more efficiently leveraging digital technologies. Prior to joining Cisco in 2018, Sielen spent 20 years at Jacobs Engineering (legacy CH2M) developing industry sector partnerships and facilitation of complex cross-business multidisciplinary teams to implement innovative and sustainable solutions for water utilities and transportation agencies. She also co-founded CH2M's Smart Cities Initiative, working in collaboration with agencies, technology leaders, and ecosystem partners. Sielen holds bachelor's and master's degrees in civil engineering from the University of Washington. She is currently serving as a coach and mentor for the Seattle Leadership Tomorrow program, a civic leadership organization focused on exploring strategies for positive change that cross sectors and silos to foster healthy communities.

Adi Karisik, Global Technology Leader, Jacobs

Adi is Jacobs' global technology leader for operational technology, with 20 years of experience in cybersecurity and intelligence, program management, ICS, and classified operations. Adi manages critical IT/OT/IoT cybersecurity projects and programs, and trains industrial clients regularly. During his 14-year tenure with Blue Canopy Group (now Jacobs), Adi served as a partner and key leader in the national security domain. His skillset includes intelligence training, predictive threat analysis, and securing locations and critical facilities. Adi has also worked within Jacobs Aerospace Technology and Nuclear Group, specifically for National Security Services for Commercial and International cyber operations. Since 2019, Adi has created and led a Jacobs-wide group aimed at OT cybersecurity. He holds a BA and MBA from Southeastern Louisiana University and has a variety of certifications and registrations in the areas of water cybersecurity, industrial cybersecurity, predictive analytics, and predictive behavioral analysis. Adi is also a certified FEMA emergency staff and is involved in AWIA assessments.

Rocky Smith, Sr. Solutions Architect for Government and Transportation, Cisco

Rocky has 20 years of experience in building, architecting, and maintaining IP networks. Rocky is the lead architect building Cisco's approach for smart water and public safety. He has an extensive background in industrial cybersecurity, working with both public and private organizations across the globe. As the lead architect for Cisco's smart water strategy, Rocky has worked closely with key players in the industrial space, including Cisco's Cyber Vision and Talos Threat Intelligence groups. As the solutions architect for the Cities and Communities team in the Industry Solutions Group at Cisco, Rocky leads the buildout of the industry-relevant architectures used worldwide by Cisco engineers and partners. Having worked at Cisco for the past 14 years, Rocky has been supporting a range of industries, including utility and energy, state, local, public safety, enterprise, K-12 and higher education, healthcare, and retail.

Glen Price, Cyber Security Consultant, Jacobs

Glen has more than 16 years of experience in design, construction, and operation of complex industrial networks for water and power utilities, transportation, mining, and oil and gas across North America, Australia, and Asia Pacific. Glen has led the successful design and implementation of multiple secure SCADA server and network solutions with multiple HMI/PLC platforms over the past 8 years. He has extensive experience with the development and application of cyber risk management frameworks to track risk over time and consequences and align treatments to those solutions, and in doing so has armed business leaders and corporate champions with the tools they need to quantify the time and cost required to address risk and apply cyber security controls to automated environments. Glen also has experience helping clients with cybersecurity policies and procedures, automation security plans, building cybersecurity programs, network vulnerability assessments and evaluations, and SCADA master planning. He holds a bachelor's degree in computer science and a master's in cybersecurity from Edith Cowan University in Australia.

Andrew McPhee, Cybersecurity/Technical Marketing Engineer, Cisco

Andrew is a technical marketing engineer for the Industrial Security team in Cisco's Security Business Group. Andrew's expertise spans across multiple industrial verticals, including water and wastewater, for assisting customers with the adoption of Cisco's leading products such as Cyber Vision for OT visibility and Identity Services Engine (ISE) for segmentation. Andrew has a bachelor's in mechatronic engineering and a master's in electronic and computer engineering from Dublin City University in Ireland, giving him a balanced understanding of operations and modernized technology. Andrew has been with Cisco for 5 years and specializes in the broader industrial security portfolio. He spent 3 of those years working in automotive networking, where he was able to demonstrate the security risks of in-vehicle networks by hacking into production vehicles.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-743927-00 07/20