Leadership for CyberBioSecurity[1]: The Case of Oldsmar Water

Case Narrative

Prepared by

Eric Kaufman[a], Samson Adeoye[a], and Feras Batarseh[b]

[a] Department of Agricultural, Leadership, and Community Education, Virginia Tech

[b] Department of Biological Systems Engineering, Virginia Tech

Author Note

Eric K. Kaufman https://orcid.org/0000-0001-8009-0066

Samson Adeoye https://orcid.org/0000-0001-9920-1539

Feras Batarseh https://orcid.org/0000-0002-6062-2747

We have no conflicts of interest to disclose. Our work was funded in part by Virginia Tech's Center for Advanced Innovation in Agriculture and the Commonwealth Cyber Initiative Southwest Virginia node through a mini-grant for Experiential Learning Development in Data Analytics and Cyberbiosecurity for Agriculture and Life Sciences.

Correspondence concerning this work should be addressed to Eric K. Kaufman, Virginia Tech Department of Agricultural, Leadership, and Community Education, 214 Litton-Reaves Hall (MC 0343), 175 West Campus Dr, Blacksburg VA 24061. Email: ekaufman@vt.edu

[1] CyberBioSecurity is an emerging field at the interface of life sciences and digital worlds. While conventionally written as "cyberbiosecurity" (or sometimes bio-cyber-security), the "bio" emphasis is central to the Cyber+Bio+Security field.

Leadership for CyberBioSecurity: The Case of Oldsmar Water

It was a Friday morning, and Ramone[2] awoke thinking about Super Bowl LV, which would be that weekend in neighboring Tampa, Florida. He didn't have tickets to the football game, but he had friends coming into town that were hoping to tailgate near the stadium. Before enjoying the weekend, though, he had to make it through his workday as a plant operator at the Water Treatment Plant in Oldsmar FL. The job involved technical work in the operation and maintenance of a Reverse Osmosis (RO) Water Treatment Plant[3]. The plant was mostly automated (Figure 1), leaving the work somewhat routine and mundane. However, today would be different. On February 5, 2021, the activities of an unknown remote hacker exposed the over 15,000 residents of Florida's west coast to potential poisoning (Bergal, 2021; FBI, CISA, EPA, & ISAC, 2021; Montgomery & Logan, 2021).

Figure 1

Photo of a Water Treatment Facility

Note. USDA Photo by Lance Cheung at https://www.flickr.com/photos/usdagov/17047828068/

At about 8:00 am, Ramone was monitoring the computer system at the water treatment plant, when he noticed that someone briefly accessed the computer remotely. However, he didn't find this unusual, because he knew his supervisor regularly accesses the system from other computers. Nothing else unusual happened until about 1:30 pm: Ramone watched his computer as someone took control of the mouse and directed the water treatment software to increase the amount of sodium hydroxide from 100 parts per million to 11,100 parts per million. Ramone immediately changed the concentration back to the correct amount and informed his supervisor of the incident. By Friday afternoon, the Pinellas

[2] The identity of the water treatment plant operator is not known publicly; "Ramone" is a pseudonym. The personalization of this character is done to help readers imagine themselves in the role of the plant operator who halted the attack.

[3] The Oldsmar Water Division provides a brief description of reverse osmosis here: https://www.myoldsmar.com/160/Water-Division

County Sheriff's office began a criminal investigation (Olsen, 2021). By Monday, United States Senator Rubio (2021) declared the incident a matter of national security (Figure 2). At a press conference on February 8th, 2021, when the Oldsmar City Manager was asked if he had heard about similar attacks at other agencies around the country, he said, "I think we anticipated that, you know, this day was coming" (10 Tampa Bay, 2021, 6:25). The Sheriff later added: "This type of hacking of critical infrastructure is not necessarily limited to just water supply systems… it could be a whole variety of things; it could really be problematic" (10 Tampa Bay, 2021, 9:53). The Oldsmar Mayor concluded, "The important thing is to put everybody on notice, and I think that's really the purpose of today" (10 Tampa Bay, 2021, 5:58).

Figure 2

Tweet from U.S. Senator About Oldsmar Water

Note. From Twitter, https://twitter.com/marcorubio/status/1358909642185890 77

Background

For over two decades the United States water system has been under different cyber threats (Holland & Magill, 2021). In 2015, the US Department of Homeland Security (DHS) responded to 25 cybersecurity incidents in the water sector, representing a 78.6% increase in the number of reported cases from 2014 (Clark et al., 2016). Cyber risks have continued to grow exponentially relative to the priority given to the water and wastewater sector, making the sector unsafe (Thryft, 2022). In March and April of 2018, the DHS and the Federal Bureau of Investigation (FBI) warned against potential cyber espionage in the US water sector by the Russian government (Germano, 2019). With the continuous automation of the water and wastewater systems, cyberattacks are a question of 'when' not 'if.'

The February 5, 2021, cyberattack on the Oldsmar water treatment plant received unusual massive public outcry as well as local water authorities' reactions and regulatory institutions' responses, causing disclosure of previously unreported attacks. While technical safeguards are available, limited sharing of information and collaboration has so far constituted security gaps and vulnerability of the water sector to cyberattacks (Hassanzadeh et al., 2020). A survey of 20,000 utility employees by the American Water Works Association (AWWA) showed that cyber threats are feared to have the highest impacts on operations, coupled with limited resources and conflicting priorities (Germano, 2019).

Water treatment plants (Figure 3) are part of water systems, which have collectively been identified as the weakest link in the US national and economic security due to lapses in cyber security awareness and preparedness (Montgomery & Logan, 2021). While technical protections have advanced in recent years, many local agencies are hampered by limited funding, particularly in the case of small facilities, like the Oldsmar water treatment plant (McKay, 2021). Furthermore, there is growing recognition that humans are the weakest link in the protection process (Ricci et al., 2019). Experts have noted that cybersecurity

Figure 3

Image of a Water Treatment Plant in Florida

Note. Photo shared by Florida Water Daily at https://flic.kr/p/sgAUdw

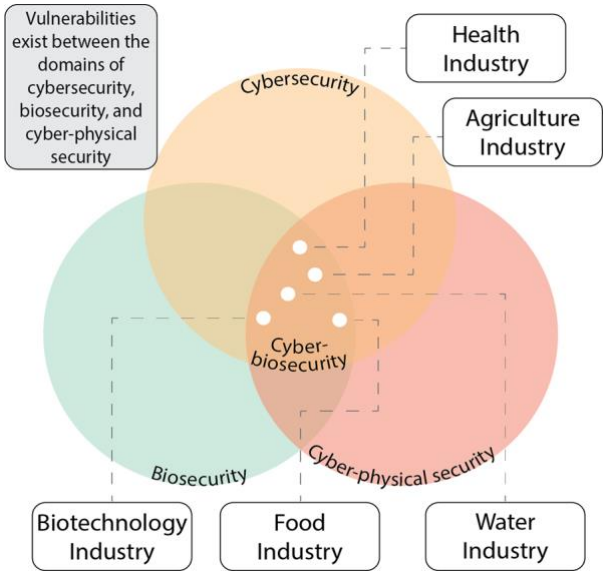
is far more than a technical problem (McShane, 2022; White, 2022). "To get it right, companies need to weave trust throughout their entire ecosystem and make security part of every job description" (Hanspal, 2021, para. 2).

While technical safeguards are available, the limited sharing and collaboration is leaving the US water supply highly vulnerable to cyber threats (Hassanzadeh et al., 2020). The Environmental Protection Agency (EPA) has oversight of more than 50,000 drinking water treatment plants and 15,000 wastewater treatment plants, but protocols for cyber security of water treatment plants have not yet been devised (CyberTalk, 2021). Because each water facility can pose unique challenges, it is unrealistic to expect the EPA to adequately protect the US water supply system. Instead, communication and collaboration is needed across a network of local water authorities, regional water resource agencies, state water control boards, etc. (The White House, 2022).

While cybersecurity experts are attuned to many conventional cyber-attacks, the overlapping challenges of biosecurity and cyber-physical security have surfaced the need for more focused attention to CyberBioSecurity (Figure 4). Attacks on the water systems transcend the direct consequential impacts of compromised drinking water and wastewater treatment on public health and the environment to the manufacturing, processing, and supply chain sectors, with grievous effects on a national scale (Montgomery & Logan, 2021). Like climate change, cybersecurity concerns are wicked problems "that are transboundary in nature, occur at multiple levels across sectors, between institutions, and will impact all actors—both public and private—in complex interconnected, and often highly politicized ways" (Carr & Lesniewska, 2020, p. 392). Addressing cybersecurity threats to biological systems (e.g., water) presents a huge task for addressing critical issues in a sector that is already battling existing wicked problems. CyberBioSecurity is a term coined to keep in focus the complex interface between the life sciences and the digital world (Murch et al., 2018), which now constitutes a significant addition to the layers of national and socioeconomic threats to the United States (Drape et al., 2021; Duncan et al., 2019; Germano, 2019).

Figure 4

Venn Diagram of Cyberbiosecurity Domains



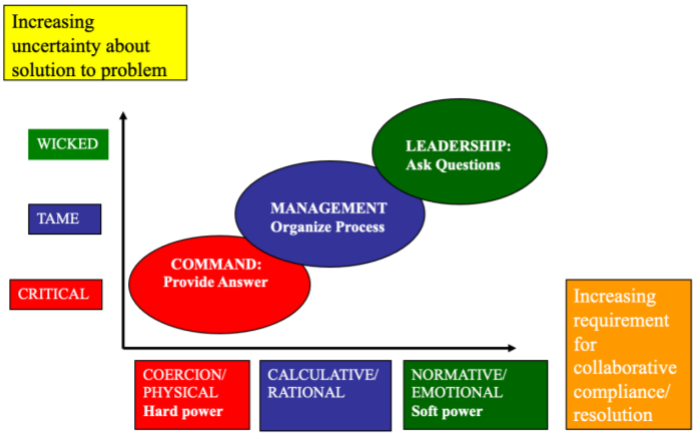
Note. Adapted from Duncan et al. (2019).

Relevance of Leadership

The world is increasingly attuned to the challenge of wicked problems (Grint, 2022). In a typology of problems, power, and authority (Figure 5), Grint (2008) distinguishes between critical, tame, and wicked problems. With increasing uncertainty about the solution to a problem, the problem moves from being categorized as critical, to tame, to wicked. In parallel, Grint (2008) argues the appropriate response is to shift from coercion (i.e., hard power) to more normative and collaborative approaches (i.e., soft power).

Figure 5

Typology of Problems, Power, and Authority



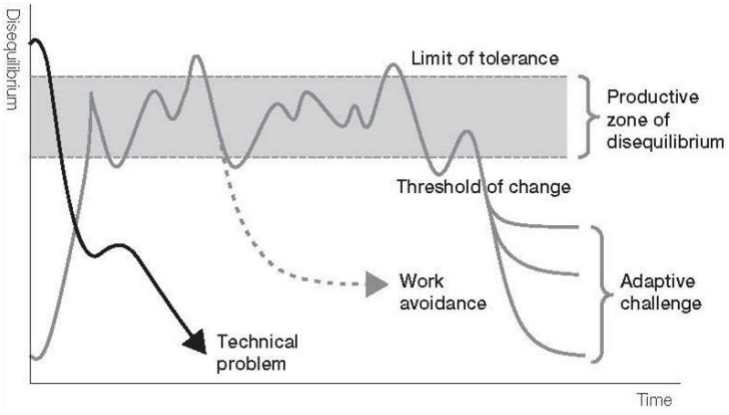
Note. From "Wicked problems and clumsy solutions: The role of leadership," by K. Grint, 2008, *Clinical Leader, 1*(2), p. 58. Copyright by Keith Grint. Reprinted with permission.

And, it is in the uncertainty and "soft power" where leadership is found. Wicked problems do not yield themselves to permanent solutions and, of course, cannot be solved by scientific or technical approaches alone. "The leader's role with a Wicked Problem, therefore, is to ask the right questions rather than provide the right answers because the answers may not be self-evident and will require a collaborative process to make any kind of progress" (Grint, 2008, p. 13). The fluid nature of technological advances means that an approach to confronting a certain CyberBioSecurity issue today might become obsolete tomorrow. Water facilities thus need to make their workforce dynamically and future-ready for CyberBioSecurity threats.

Complementary to Grint's (2008) typology of problems, Heifetz et al. (2009) encourage application of adaptive leadership. Summarized by Northouse (2022), "Adaptive leadership focuses on the *adaptations* required of people in response to changing environments" (p. 285). In order to sustain engagement in the work of adaptive leadership, Heifetz et al. (2009) suggest commitment to a "productive zone of disequilibrium" (Figure 6). However, there is a tendency to focus on the technical problem at hand and avoid the longer-term adaptive challenge(s). The reason for the skewed interest in technical solutions can be attributed to the fact that adaptive challenges are difficult, requiring changes in people's held assumptions, beliefs, attitudes, and behaviors, which require Leadership-

Figure 6

Productive Zone of Disequilibrium for Adaptive Leadership



Note. Reprinted from R. A. Heifetz, A. Grashow, & M. Linsky, 2009, *The theory being the practice: A brief introduction to the adaptive leadership framework*, p. 18. Copyright 2009 by Harvard Business Press.

as-Practice Development (LaPD) (Northouse, 2022; Raelin, 2016). This poses the question of how the current and future workforce at the interface of the life science and digital world can be able to confront CyberBioSecurity concerns – a wicked problem – with only technical solutions.

The resultant uncertainty in the world of work from the foregoing is not far-fetched. The Prince's Trust (2022) showed that despite high percentages of young people interested in agricultural-related and digital jobs, one out of every three believes their education lacks relevant skills needed for the workplace – which is increasingly becoming more adaptive than technical. There is urgency in filling this educational and workforce gap, as cyber-terrorism, for example, in life science industries is rapidly increasing, causing threats to our food and water supply and public health systems (Drape et al., 2021; McDonald, 2021; Pauwels, 2020). Moreover, cyberattacks on water systems expose other critical infrastructures like energy and electricity generation to disruptive and cascading effects – potentially making water the weakest link in the US national and economic security (Montgomery & Logan, 2021). These disruptive and cascading effects are the results of intertwining issues within and beyond discrete disciplines and sectors – typical of wicked problems.

A wicked problem – in this case CyberBioSecurity – "is more complex, rather than just complicated – that is, it cannot be removed from its environment, solved, and returned without affecting the environment. Moreover, there is no clear relationship between cause and effect … there cannot be a scientific [or technical] solution to the problem …" (Grint, 2008, p. 12, bracketed phrase added). The reality created by the long haul in dealing with this kind of challenge and the accompanying uncertainties is a leadership concern. Confronting this challenge requires the effort of the collective, where the individual leader transfers authority to the collective, contrary to traditional leadership (Grint, 2008); and leadership-as-practice development enshrines this collective model (Raelin, 2016). This case study sets to inspire a hybrid leadership philosophy that encapsulates adaptive leadership in leadership-as-practice for dealing with wicked problems.

Key Players

Achieving intersectoral and cross disciplinary collaboration is not easy; it requires engagement of a wide variety of stakeholders (Figure 7). Some of the key players are identified here.

Figure 7
CyberBioSecurity Involves Many Stakeholders

Plant Operator: A person that monitors and maintains water plant equipment. This person observed the activities of the hacker during the Oldsmar plant cyber-attack and promptly reversed the malicious alterations in the industrial control system. Because the Oldsmar plant operator's name is unknown, this case narrative refers to the plant operator with a pseudonym (i.e., Ramone).

Plant Supervisor: The line manager to the plant operator and other subordinate workers of similar rank. Different departments/units like engineering, Information and Communication Technology (ICT), reverse osmosis, customer service, water quality assurance, etcetera, have supervisors responsible for different monitoring and coordination activities.

Plant Administrator: The overall plant executive officer. Responsible for the coordination of the various departments/units towards the goals of supplying safe water to the public and preventing environmental hazards.

City Manager: An executive responsible for the day-to-day running of a city in the United States. They bring public service to the people by bridging the gap between politics and administration. In 2021, the City Manager of Oldsmar was Al Braithwaite, and he made public addresses following the Oldsmar water plant attack, informing the public of the incidence and mitigation steps taken.

Mayor: An elected official and head of the municipal council. Directs and supervises the administrative structure of government departments within a city and is generally responsible for appointing and removing department heads. The City Manager is responsible to the City Council, which is headed by the mayor. The Oldsmar Mayor, Eric Seidel, was seen to work with the County Sheriff and the Oldsmar City Manager to address the public on issues on the water plant attack at Oldsmar.

Sheriff: An elected county officer responsible for peacekeeping and law enforcement within a county or other civil sub-divisions of a state. Directly accountable to the citizens; focused on work to ensure their safety. The Pinellas County Sheriff, Bob Gualtieri, spoke at a press conference following the Oldsmar water attack in the company of the Oldsmar City Manager and the Oldsmar Mayor.

Federal Bureau of Investigation (FBI): The United States federal law enforcement agency in charge of investigating and preventing acts of domestic and international terrorism. The FBI is the lead agency for investigating cyber-attacks.

Cybersecurity and Infrastructure Security Agency (CISA): U.S. Government institution responsible for enhancing the security, resilience, and reliability of cybersecurity and communication infrastructure.

Environmental Protection Agency (EPA): An agency of the United States working to protect human health and the environment by ensuring clean air, land, and water.

National Security Agency (NSA): An agency of the US government saddled with the mandate to prevent and eradicate threats to the country's national security systems with particular attention to the Defense Industrial Base and promotion of cybersecurity education, research, and career-building.

Status Report

The cyber-attack on the Oldsmar water plant raised both public and industry awareness of the potential threat(s), with many points summarized in an entry in *The Cybersecurity Almanac* (Appendix A). State and local officials throughout the country issued cyber alerts and advisories/policies to their water utilities, and some have opted to offer additional training for staff and focus on cybersecurity during their oversight functions (Bergal, 2021). Recommendations abound for technical solutions (CISA, n.d.;

FBI, CISA, EPA, & NSA, 2021; Appendix A). However, inadequate funding/budgeting and/or staffing has been identified as a limiting challenge to proactively building sustainable operational systems (Foundation for Defense of Democracies [FDD], 2022). Public analysts and IT experts have been critical of the state of sophistication of the software being used. Kardon (2021) believes that the attack "could have been prevented with more securely configured remote engineering access." Kardon also blames the incident on Oldsmar's allowing of remote access into its industrial control system (ICS) with TeamViewer, an insecurely configured, and likely unauthorized, software.

Al Braithwaite, the Oldsmar City Manager, reported that the compromised system that allowed the cyber intrusion has been disabled and system upgrades initiated. Other regional water facilities have also taken related steps, perceived to strengthen their systems against intrusion. Water utilities across the United States (including approximately 52,000 potable water and 16,000 wastewater systems) are unique in many technological, personnel, and environmental perspectives, and currently operate independently in a decentralized manner (FDD, 2022). The FDD (2022) asserts that "conducting federal oversight of, and providing sufficient federal assistance to, such a distributed network of utilities is inherently difficult" (para. 1). Following the Oldsmar attack, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Agency (CISA), the Environmental Protection Agency (EPA), and the National Security Agency (NSA) (2021) released a joint cybersecurity advisory that highlights various dynamics of, and prevention and mitigation approaches to cyberattacks on the operational technology (OT) and information technology (IT) components of the U.S. Water and Wastewater Systems (WWS) facilities by highlighting common tactics, techniques, and procedures (TTPs) that "threat actors" use to make IT and OT networks and systems vulnerable. President Joe Biden's administration is expanding the public-private cybersecurity partnership to the water sector through the extension of the Industrial Control Systems (ICS) Cybersecurity Initiative (The White House, 2022). The White House also noted that a Water Action Plan was developed in partnership with EPA, CISA, and the Water Sector Coordinating Council (WSCC), representing the federal government's collaborative effort with the critical water infrastructure community to enhance "the deployment of technologies and systems that provide cyber-related threat visibility, indicators, and warnings" (The White House, 2022, para. 3). These three stakeholders (i.e., EPA, CISA, WSCC) are saddled with the responsibility to "collaborate to promote cybersecurity monitoring to the entire sector" (The White House, 2022, para. 5), while EPA and CISA will specifically work with water utilities to develop protocols for information sharing. The EPA (2022) summarize the action plan as follows:

> The *Water and Wastewater Sector Action Plan* focuses on promoting and supporting the water sector's adoption of strategies for the early detection of cyber-threats and allow for the rapid sharing of cyber-threat data across the government in order to expedite analysis and action. Actions include:
> - Establishing a task force of water sector leaders.
> - Implementing pilot projects to demonstrate and accelerate adoption of incident monitoring.
> - Improving information sharing and data analysis.
> - Providing technical support to water systems. (para. 4)

The over 68,000 water systems are unique in many ways and a realistic action plan will need to incorporate this uniqueness. This poses a challenge to centralized control of the water systems. Individual water utilities will have to build adaptive capacity in order to achieve local, regional, and national security of the United States water systems in both the short and long terms.

Case Problem(s)

Challenge #1: Analyzing Technical and Adaptive Challenges

Explore details of threats to the water infrastructure in the United States. Using the worksheet in Appendix B, describe the technical challenges, the adaptive challenges, and those that are both technical and adaptive. Then, considering responses to the Oldsmar water attack, summarize the adaptive leadership to date, aligning the summary with the four A's of adaptive leadership (Ramalingam et al., 2020): Anticipation, Articulation, Adaptation, and Accountability. Prepare a brief presentation with a slide for each of the four A's (Appendix C).

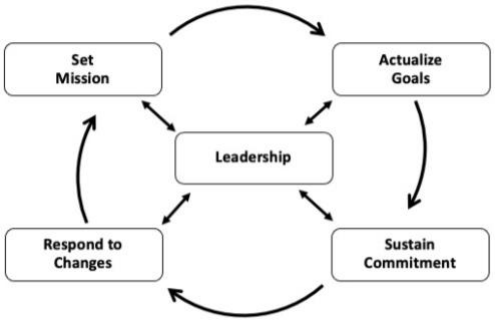
Challenge #2: Preparing Practical Recommendations

Imagine you are a consulting group that has been hired by the West Virginia American Water (WVAW) to provide practical recommendations for mitigating risks from the ongoing cyber threats to water systems. The consulting contract is being funded in part by recent federal government investments to improve water infrastructure in rural West Virginia (USDA, 2022). Since its creation in 1886, WVAW has undergone many transitions and worked to stay current with technology, including appropriate safeguards (Aaron, 2021). The WVAW administrator has expressed concerns over maintaining the longstanding values of WVAW—safety, trust, environmental leadership, teamwork, and high performance—in the face of cyber threats on water systems across the country. Considering the adaptive challenges associated with CyberBioSecurity, WVWA is particularly interested in recommendations associated with the critical leadership processes associated with leaderful organizations (Figure 8; Raelin, 2005). The immediate task is to outline a report that incorporates recommendations aligned with a leadership-as-practice (L-A-P) approach (Raelin 2016). Use the worksheet in Appendix D to highlight L-A-P activities for consideration.

Challenge #3: Connecting Leadership for CyberBioSecurity to Other Contexts

Using the Internet to explore current events, identify other contexts where leadership for CyberBioSecurity is needed. For example, in May 2022, Russian troops' theft of tractors in Ukraine was thwarted by remote disabling of those tractors (Roberts, 2022), but that revelation has sparked new concerns about systemic risks to agriculture. While many farmers have advocated for the "right to repair" their computerized equipment (Newman, 2022), the agriculture community has historically been slow to appreciate the cyber threats (Grispos & Doctor, 2022). If you were asked to present to a group of farmers regarding improved strategies for CyberBioSecurity, what would you highlight? What other groups need to hear similar messages in order to advance protections?

Figure 8
Critical Processes of Leadership



Note. Adapted from "Creating Leaderful Organizations: How to Bring Out Leadership in Everyone," by J. A. Raelin, 2003, p. 7.

References

Aaron, B. (2021, February 10). *Local officials aware of potential cyber threat to water system*. WCHS News. https://wchstv.com/news/local/local-officials-aware-of-potential-cyber-threat-to-water-system

Bergal, J. (2021, March 10). *Florida hack exposes danger to water systems* [Stateline Article]. The Pew Charitable Trusts. https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems

Carr, M., & Lesniewska, F. (2020). Internet of Things, cybersecurity and governing wicked problems: Learning from climate change governance. *International Relations, 34*(3), 391-412. https://doi.org/10.1177/0047117820948247.

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

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *Cyber essentials toolkits*. https://www.cisa.gov/publication/cyber-essentials-toolkits

CyberTalk.org. (2021, November 19). *Protecting America's water supply: The latest threats…*. https://www.cybertalk.org/2021/11/19/protecting-americas-water-supply-the-latest-threats/

DeWalt, D., McAlpine, E., Tedesco, M., Skirbe, K., Boukouris, D., Krongold, A., McDowell, C., & Sztejnberg, A. (2022). *The cybersecurity almanac, 2022*. Momentum Cyber. https://momentumcyber.com/docs/Yearly/2022_Cybersecurity_Almanac_Public_Edition.pdf

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R. S., & Duncan, S. E. (2021). Assessing the role of cyberbiosecurity in agriculture: A case study. *Frontiers in Bioengineering and Biotechnology*, *9*, 737927. https://doi.org/10.3389/fbioe.2021.737927

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system. *Frontiers in Bioengineering and Biotechnology, 7*, 63. https://doi.org/10.3389/fbioe.2019.00063

Environmental Protection Agency (EPA). (2022, January 27). *EPA announces action plan to accelerate cyber-resilience for the water sector* [News release]. https://www.epa.gov/newsreleases/epa-announces-action-plan-accelerate-cyber-resilience-water-sector

Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Agency (CISA), Environmental Protection Agency (EPA), & Multi-State ISAC. (2021, February 11). Compromise of U.S. Water Treatment Facility. *Joint Cybersecurity Advisory, AA21-042A.* https://www.cisa.gov/uscert/sites/default/files/publications/AA21-042A_Joint%20Cybersecurity%20Advisory_Compromise%20of%20U.S.%20Water%20Treatment%20Facility.pdf

Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Agency (CISA), Environmental Protection Agency (EPA), & National Security Agency (NSA). (2021, October 14). Ongoing cyber threats to U.S. Water and Wastewater Systems. *Joint Cybersecurity Advisory, AA21-287A.* https://www.cisa.gov/uscert/sites/default/files/publications/AA21-287A-Ongoing_Cyber_Threats_to_U.S._Water_and_Wastewater_Systems.pdf

Foundation for Defense of Democracies (FDD). (2022, June 8). *Strengthening the cybersecurity of American water utilities*. https://www.fdd.org/events/2022/06/08/strengthening-the-cybersecurity-of-american-water-utilities/

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

Grint, K. (2008). Wicked problems and clumsy solutions: The role of leadership. *Clinical Leadership, 1*(2), 11-15. http://leadershipforchange.org.uk/wp-content/uploads/Keith-Grint-Wicked-Problems-handout.pdf

Grint, K. (2022). Critical essay: Wicked problems in the age of uncertainty. *Human Relations, 75*(8), 1518–1532. https://doi.org/10.1177/00187267211070770

Grispos, G., & Doctor, A. C. (2022, August 8). *Rise of precision agriculture exposes food systems to new threats*. The Conversation. https://theconversation.com/rise-of-precision-agriculture-exposes-food-system-to-new-threats-187589

Hanspal, L. (2021, January 6). *Cybersecurity is not (just) a tech problem.* Harvard Business Review. https://hbr.org/2021/01/cybersecurity-is-not-just-a-tech-problem

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

Heifetz, R. A., Grashow, A., & Linsky, M. (2009). *The theory behind the practice: A brief introduction to the adaptive leadership framework*. Harvard Business Press. https://www.hbsp.harvard.edu/product/3241BC-PDF-ENG

Holland, J., & Magill, B. (2021, February 10). *Water plant cyberattack is wake up call, 20 years in the making*. Bloomberg Law. https://news.bloomberglaw.com/privacy-and-data-security/water-plant-cyberattack-raises-critical-infrastructure-concerns

Kardon, S. (2021, February 9). *Florida water treatment plant hit with cyber attack*. Industrial Defender. https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/

McDonald, M. (2021). *SAFE with cyberbiosecurity: Protecting the agriculture and food system*. Commonwealth Cyber Initiative. https://cyberinitiative.org/cci-news/2021/cyberbiosecurity.html

McKay, J. (2021, February 19). *Water treatment facility cyberattack suggests more to come.* Government Technology. https://www.govtech.com/em/safety/cyberattack-on-water-treatment-facility-suggests-more-to-come.html

McShane, I. (2022, June 19). *Why cybersecurity is also a human issue, not just a technology one*. TechNative. https://technative.io/why-cybersecurity-is-also-a-human-issue-not-just-a-technology-one/

Montgomery, M., & Logan, T. (2021). *Poor cybersecurity makes water a weak link in critical infrastructure*. Foundation for Defense of Democracies (FDD), Center on Cyber and Technology Innovation (CCTI). https://www.fdd.org/analysis/2021/11/18/poor-cybersecurity-makes-water-a-weak-link-in-critical-infrastructure/

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology*, *6*, 39. https://doi.org/10.3389/fbioe.2018.000

Northouse, P. G. (2022). *Leadership: Theory and practice* (9th ed.). Sage.

Olsen, J. (2021, February 8). *'This is dangerous stuff': Hacker increased chemical level at Oldsmar's city water system, sheriff says*. 10 Tampa Bay, WTSP. https://www.wtsp.com/article/news/local/pinellascounty/pinellas-oldsmar-water-system-computer-intrustion/67-512b2bab-9f94-44d7-841e-5169fdb0a0bd

Pauwels, E. (2020, June 18). *What's needed to prevent cyberbiosecurity threats and protect vulnerable countries*. World Economic Forum. https://www.weforum.org/agenda/2020/06/prevent-cyber-bio-security-threats-covid19-governance/

Raelin, J. A. (2003). *Creating leaderful organizations: How to bring out leadership in everyone*. Berrett-Koehler Publishers.

Raelin, J. A. (2005). We the leaders: In order to form a leaderful organization. *Journal of Leadership & Organizational Studies*, *12*(2), 18-30. https://doi.org/10.1177/107179190501200202

Raelin, J. A. (2016). Introduction to leadership-as-practice: Theory and application. In J. A. Raelin (Ed.), *Leadership-as-practice: Theory and application* (pp. 1-17). Routledge. https://doi.org/10.4324/9781315684123-1

Ramalingam, B., Nabarro, D., Oqubay, A., Carnall, D. R., & Wild, L. (2020, September 11). 5 principles to guide adaptive leadership. *Harvard Business Review*. https://hbr.org/2020/09/5-principles-to-guide-adaptive-leadership

Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies, 24*, 231–249. https://doi.org/10.1007/s10639-018-9765-8

Roberts, P. (2022, May 3). *Feel good Ukraine tractor story highlights ag cyber risk*. The Security Ledger. https://securityledger.com/2022/05/feel-good-ukraine-tractor-story-highlights-ag-cyber-risk/

Rubio, M. (2021, February 8). *I will be asking the @FBI to provide all assistance necessary in investigating an attempt to poison the water supply of a #Florida city. This should be treated as a matter of national security* [Thumbnail with link attached] [Tweet]. Twitter. https://twitter.com/marcorubio/status/1358909642185859077

The Prince's Trust. (2022). *An upskill struggle: Supporting a generation of untapped potential*. https://www.princestrustglobal.org/upskill-struggle

The White House. (2022, January 27). *Fact sheet: Biden-Harris administration expands public-private cybersecurity partnership to water sector* [Statements and Releases]. https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/27/fact-sheet-biden-harris-administration-expands-public-private-cybersecurity-partnership-to-water-sector/

Thryft, A. R. (2022, July 20). *U.S. Water sector cybersecurity: "Absolutely inadequate."* EE Times. https://www.eetimes.com/u-s-water-sector-cybersecurity-absolutely-inadequate/

U.S. Department of Agriculture (USDA). (2022, August 31). *Biden-Harris administration invests $75 million to provide clean drinking water and safe wastewater infrastructure in rural West Virginia* [Press release]. https://www.usda.gov/media/press-releases/2022/08/31/biden-harris-administration-invests-75-million-provide-clean

White, L. (2022, May 4). *Why cybersecurity isn't just tech's problem - it's HR's*. Human Resource Director. https://www.hcamag.com/ca/specialization/hr-technology/why-cybersecurity-isnt-just-techs-problem-its-hrs/404744

Appendix A: Oldsmar Case Entry in *The Cybersecurity Almanac* (DeWalt et al., 2022, p. 106)

Municipal Water Treatment Attack: OLDSMAR FL

Threat Actors Leveraged TeamViewer To Access A Water Treatment Plant's Controls To Modify Lye Concentration.

Bruce T. Haddock Water Treatment Plant | Incident Overview

Background

Assumed Motive:	Poison the town residents by raising the lye content of water from 100 ppm to 11,100 ppm
Point of Entry:	Identical User Passwords / TeamViewer VM
Target:	OLDSMAR FL Bruce T. Haddock Water Treatment Plant

Attack Overview / Timeline

- On February 5, 2021 unknown hackers accessed a computer system that was used as a **remote control** for the Bruce T. Haddock Water Treatment Plant
- The threat actors likely accessed the system by exploiting passwords that had been leaked on the dark web, and accessed the network which had no firewall security
- The control system for the plant was accessed via the **VM TeamViewer** that enabled remote controls for the plant
- Threat actors increased the amount of lye in the water by more than **100x** to potentially dangerous levels
- An employee realized the system was compromised, when he saw his desktop mouse moving, and reversed the levels of lye within the water; it would have taken **24-36** hours for the contaminated water to circulate

Attacker Profile & Methodology

Attacker Profile	▪ Unidentified individual / group using noisy & haphazard techniques which points to a less sophisticated actor ▪ There is not enough information to identify who caused the attack, but FBI and Secret Service are still investigating
Assumed Motives	▪ Full attack rationale is unknown; the actions during the attack point to a deadly intent ▪ Contaminate Oldsmar, Florida's water supply, poisoning residents and disabling the water treatment plant
Method	▪ Connected to the SCADA system, which was accessible through a single password used by all employees ▪ Leveraged TeamViewer to access system controls and manipulate lye content to extreme levels
Potential Ramifications	▪ Could act as a catalyst for other threat actors to target infrastructure with weak security measures ▪ Demonstrates the ease at which some pieces of infrastructure can be breached and manipulated

Avoided Fallout

Lye, or sodium hydroxide, is a **caustic** substance and can cause **chemical burns** to the skin or internal **corrosive damage** if ingested

If the concentration change had gone undetected, it could have resulted in the **mass poisoning** of Oldsmar, a town of **15,000** people

IT / OT Security Issues & Recommended Remediation

Industry Challenges

The OT space faces increasing **vulnerabilities** through the convergence of IT & OT environments, **compromising** the traditional security of the air gap technique used to isolate separate domains

2,000%
Increase in OT attacks from 2019 to 2020

90%
organizations experienced **at least one** OT system intrusion in 2020

33%
Of OT attacks in 2020 were committed via Ransomware

15%
Of OT attacks in 2020 were attributed to Remote Access Trojans (RAT)

Why Cybersecurity In Infrastructure Matters

SCADA Breaches	Recently, threat actors have been distributing access to SCADA and ICS systems on dark web markets, which are increasingly vulnerable to attacks
Digital Transition	It is expected that the number of internet connected devices will double through 2025 increasing the attack surface for critical infrastructure
Debilitating Outcomes	The potential consequences of a successful attack on critical infrastructure could disrupt other essential systems and entire industries

Infrastructure Security Best Practices

VPN & Firewall	Enable bidirectional communication between IT & OT environments, best deployed in a demilitarized zone for a secured and regulated access protocol
Network Segregation	Ensure employees are extended access to only the systems they need, and place systems on separate networks with privileged access
Unidirectional Gateways	Extract & send key information, while preventing inbound communication from OT environments without opening critical systems to unwanted infiltration

Source: Company Press Releases, Public Press Releases, Axios: Mass Florida Poisoning; Bank Info Security: Water Treatment Hack; C&EN: Water Treatment Hack Effects; Forbes: Old Software & Password Exploit; Fortinet: State of OT Security; Gartner: OT Best Practices; IBM: X-Force Index; Reuters: Cyber Florida Hack; ZDNet: Hacker Modifies Chemicals;

Reprinted from *The Cybersecurity Almanac* (DeWalt et al., 2022, p. 106), published at https://momentumcyber.com/

Appendix B: Matrix of Technical vs. Adaptive Challenges

Instructions: Use this worksheet to identify both technical and adaptive challenges associated with this case study. Challenge yourself to enter information in all three boxes.

Technical Challenges: (The problem and solution are both clear, and the work to be done lies with a particular authority.)	**Adaptive Challenges:** (The problem and solution both require learning, and the work to be done lies with stakeholders.)
Technical and Adaptive Challenges: (The problem is clear, but the solution requires learning. The work to be done lies both with an authority and stakeholders.)	

Appendix C: Attending to the Four A's of Adaptive Leadership

Instructions: Use this worksheet to summarize observations associated with the four A's of adaptive leadership (Ramalingam et al., 2020): Anticipation, Articulation, Adaptation, and Accountability.

Anticipation of likely future needs, trends and options.	**Articulation** of these needs to build collective understanding and support for action.
Adaptation so that there is continuous learning and the adjustment of responses as necessary.	**Accountability**, including maximum transparency in decision making processes and openness to challenges and feedback.

Appendix D: Exploring Activities of Leadership-as-Practice

Instructions: Use this worksheet to highlight activities to be found in leadership-as-practice (Raelin, 2016) and incorporated into specific recommendations for action.

Scanning (Identifying resources, such as information or technology, that can contribute to new or existing programs through simplification or sensemaking.)

Signaling (Mobilizing and catalyzing the attention of others to a program or project through such means as imitating, building on, modifying, ordering, or synthesizing prior or existing elements.)

Weaving (Creating webs of interaction across existing and new networks by building trust between individuals and units or by creating shared meanings to particular views or cognitive frames.)

Stabilizing (Offering feedback to converge activity and evaluate effectiveness, leading, in turn, to structural and behavioral changes and learning.)

Inviting (Encouraging those who have held back to participate through their ideas, their energy, and their humanity.)

Unleashing (Making sure that everyone who wishes to has had a chance to contribute, without fear of repercussion, even if their contribution might create discrepancy or ambiguity in the face of decision-making convergence.)

Reflecting (Triggering thoughtfulness within the self and with others to ponder the meaning of past, current, and future experience to learn how to meet mutual needs and interests.)
