
Fall 2021 Issue | Volume 10 | Number 30
United States
{CYBERSECURITY}
Magazine
www.uscybersecurity.net

From the Fall 2021 Issue
Cybersecurity & Critical Infrastructure

What is Cyber Leadership?

Diane M Janosek, Esq., CISSP
Senior Legal Advisor | WiCyS Mid-Atlantic

The Case Study of the 2021 Hacking of a Florida Water Treatment Plant

We often hear “cyber” and often hear “leadership”. So, what is “cyber leadership” and how is it any different than leading any other senior position in business?
First, let us define cyber as a noun with both tangible and intangible aspects. Cyber is the catch-all for information and data traversing digitally across the globe.

… but cyber is really a combination of three parts:

1. Technology and digital infrastructure often referred to in shorthand as IT (Information Technology);
2. People (the professionals working in the discipline and their critical thinking skills); and third,
3. Processes that define roles and responsibilities (these processes would include technical controls, administrative controls, and physical controls).

Yes! “Cyber” is the intersection of IT, People, and Processes. The challenge is that there cannot be any gaps in the seams of these three elements – that is where cyber leadership comes into play.

CASE STUDY:

Let’s use a current event to describe “cyber.” Then, we can extrapolate and define what cyber leadership is. In Florida, in February 2021, there was a cyber-attack on a small water treatment facility. If cyber consists of three parts, what were they here? And how could cyber leadership have made a difference? This article explores the hacking incident on a resource we all value – water – and applies cyber leadership traits to assess lessons learned.

The three parts of “cyber” in the Florida water treatment facility hack are as follows:

1. The digital infrastructure and physical infrastructure of the Florida water treatment plant and its operational technology. (Technology)
2. The teammates and employees working at the plant, to include the engineers on-site and remotely, who support its operations. (People)

3. The processes involved with a water treatment facility includes: (Processes)

    - Physical barriers, security, and alerts for physical breaches,
    - Processes in place to direct chemical usage and water levels, and
    - Oversight mechanisms in place to manage daily operations and quality controls (i.e., physical controls, technical controls, and administrative controls).

So, what were the facts? What happened? What went wrong that water levels were attempted to be altered to a dangerous highly corrosive level for human consumption?

FACTS (AS REPORTED):

- Oldsmar, Florida’s water treatment plant serviced 15,000 people in the region with safe drinking water.

- This treatment plant is just one of 50,000 community water systems in the United States.

- Most Americans across the country are serviced by 10,000 community water systems, with 40,000 smaller facilities servicing less than 3,300 customers each.

- On February 5, 2021, in Oldsmar, Florida, in Pinellas County, an engineer detected that a bad actor accessed the facility's control system. The hacker attempted to increase the amount of lye used to treat the water to dangerously high levels.

- Lye was increased from 100 parts per million to 11,100 parts per million, so by a factor of more than 100.

- Lye is sodium hydroxide and is used to control acidity of water; it is very corrosive and is found in household cleaning products.

- The water treatment plant engineer witnessed this change at 8:00am on a Friday. He reversed it and assumed it was an error of a remote co-worker.

- The same engineer then witnessed it happening again at 1:30 pm when he realized his mouse was being externally or remotely controlled. He waited to regain control of the mouse and then reversed the chemical increase.

- He immediately informed his supervisory chain, and local legislative officials called in the FBI to investigate.

WHAT WENT WELL:

- **Technology and Risk Mitigation**: The Oldsmar, Florida facility had conducted an EPA recommended review of its plant for safety and cybersecurity in 2020. This review revealed weaknesses and needed corrective action. Also, this review was not required due to their small size under the EPA regulation.

- **People:** The water treatment plant had conscientious employees and they acted swiftly.

- **Processes:** The plant reported that if the engineer was not there, there was a technology control that would have prevented the lye from increasing within about 24 hours.

WHAT WENT NOT SO WELL:

- **Technology and Risk Mitigation**:
    - While the Oldsmar, Florida facility conducted an EPA review for safety and cybersecurity in 2020, and even though they identified vulnerabilities, no corrective action or mitigation had yet taken place.
    - The hacker gained access through TeamViewer remote access software; and all computers shared the same password for remote access.
    - The 32-bit version of Windows 7 operating system was in use and needed updating.
    - The system was connected to the internet without firewall protection.
- **People:** The team members should have known or have been trained more frequently on basic cyber best practices, and aware of never using shared passwords, aware of firewall protection and monitoring installation, and the importance of updating operating systems.
- **Processes:** While the water treatment plant strove to increase telework during the pandemic, the new software and pertinent plan processes needed to be updated to adhere to the same requirements it had to limit physical plant access. TeamViewer remote access software is not necessarily a vulnerability if it is installed and used appropriately as part of layered access, credentialing, and two-factor authentication.

WHAT CAN WE LEARN ABOUT CYBER LEADERSHIP FROM THIS CASE STUDY?

The most important and simplistic takeaway is that cyber leadership will always require the senior manager to assess and consider the three parts as one system and to recall that each part is of equal weight, and one part should never be reviewed or mitigated in isolation.
When evaluating unknowns as part of a risk analysis and decision matrix, consider technology, people and processes. A Cyber Leader will appreciate that:

1. **Technology and Risk Assessment:** All technology, once connected to a business or operational system, will introduce both functionality

and risk. Cyber Leaders will appreciate the various approaches to cybersecurity risk strategy, comprehend current and emerging technology, appreciate threat trends on the horizon, and then have the skill set to accurately assess and manage risk, as well as clearly communicate the technology and risk mitigation strategy.

2. **People**: People are a key component to cybersecurity, and studies have revealed that employees usually are the 'weakest link." A Cyber Leader will understand how senior executives need to impress the value of updated frequent training and professional development, as well as encouraging employees to acquire new knowledge and cyber threat awareness. People absolutely impact an effective security strategy (or not) of a business, school or organization, so a Cyber Leader will invest in talent and learning.

3. **Processes: Comprehension of** a process review includes evaluating all critical functions and components of information security, network security, network configurations, and their dependencies. This process review must also include reviewing all relationships to include third-party providers and partners, data storage repositories and locations, sensitivity and/or criticality of the data, as well as existing methods in place to mitigate the likelihood of any breaches. This complete process should take place on a consistent and regular basis to reduce probability and severity of future cyber-attacks.

Cybercrime is out there, but it is not to be feared; it can be managed and limited. As U.S. President Harry S. Truman said, *"America was not built on fear. America was built on courage, on imagination, and an unbeatable determination to do the job at hand."* President Truman created the National Security Agency in 1952, and he respected the challenges and complexity of information security to our national defense and future prosperity.

We can learn from his vision and accept his charge!
Cybersecurity professionals, we've got this! Courage. Imagination. Determination.

Resources:

1. Evans, Jack. “Someone tried to poison Oldsmar’s water supply during hack,” *Tampa Bay Times*, Feb. 9, 2021.
2. Naraine, Ryan. “U.S. Government Warning on Supply Hack: Get Rid of Windows 7,” *SecurityWeek,* Feb. 12, 2021.
3. Smith, Rebecca. “Water Systems Have Few Defenses for Hacks,” *Wall Street Journal*, A3, Feb. 13, 2021.
4. “Water treatment cyberattack.” *The Cyberwire, The Week that Was*, Feb. 13, 2021.

Author: Diane M Janosek, Esq., CISSP

Ms. Diane M. Janosek is a member of Defense Intelligence Senior Executive Service and is the National Security Agency’s Training Director and Commandant of the National Cryptologic School, comprised of the Colleges of Cyber and Cryptology. She is a multiple award recipient receiving 2020 Cyber Impact Award, Top 100 Women in Cybersecurity 2020, CybHER 2020 Warrior, and 2019 Cyber Warrior Woman of the Year. She founded both Women in Cybersecurity’s (WiCyS) Mid-Atlantic & WiCyS Critical Infrastructure.