



1

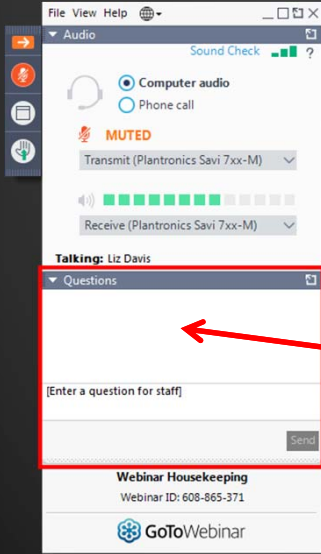
**Cyber Security for  
Non-Technical Managers**

Thursday, August 22, 2019  
1:00 - 2:30 PM ET

The Water Environment Federation logo is located in the bottom right corner of the slide. It features the same stylized 'W' icon and text as seen in the first image.

2

## How to Participate Today



- Audio Modes
  - Listen using Mic & Speakers
  - Or, select "Use Telephone" and dial the conference (please remember long distance phone charges apply).
- Submit your questions using the Questions pane.
- A recording will be available for replay shortly after this webcast.

Water Environment Federation  
the water quality people

3

## Today's Moderator:



Philip Tiewater, P.E.  
Asset Management Evangelist



4

## In 2019...

- City of Greenville, North Carolina, had to disconnect most city-owned computers from the Internet due to what officials said was a RobinHood ransomware infection, a duplicitous piece of malware that pretends to raise awareness and funds for the people of Yemen.
- Imperial County, California was hit with Ryuk ransomware, which is designed to target enterprise environments, forcing its website to go dark and causing some city systems to malfunction, including a number of departments' phone lines.
- City of Stuart, Florida, was hit by Ryuk ransomware, forcing system shut-downs affecting payroll, utilities and other vital functions, including police and fire departments.
- The municipally owned airport in Cleveland, Ohio, Cleveland Hopkins International airport, was struck by still-unspecified malware, causing the airport's flight and baggage information boards to go dark, an outage that lasted at least five days.



5

## ...more small cities...

- Riviera Beach City, Florida -- population 34,000 -- paid \$600,000 in bitcoin to hackers after data and services were lost to a ransomware attack.
- Lake City, Florida -- population 12,000 -- paid a ransom of \$500,000 after ransomware took down almost all of the city council's IT services and systems.
- Jackson County, Georgia -- population 70,000 -- was also hit by a ransomware attack and officials paid \$400,000 to regain access to IT systems.



6

## ...and big cities

- Atlanta (\$2.7 million)
- Baltimore (\$18.2 million)
- Los Angeles (20k personal files)
- Newark (\$30k ransom)



7

## ...and even a state DOT

- Colorado DOT



8

## Cyber security is everyone's job

- Passwords
- Phishing
- Public Wi-fi
- Update software



9

## Panelists

- Sue Schneider & Kevin Brown, Spartanburg Water
- Elkin Hernandez, DCWater
- John Sudduth, Metropolitan Water Reclamation District of Greater Chicago



10

## Our Next Speakers:



Sue Schneider  
*CEO*



Kevin Brown  
*Director of IT*

*Spartanburg Water*  
Spartanburg, SC



11

## A CEO's Perspective on Cyber Security



12

## What are our Day to Day Technology Challenges ?

- Exceed Customer Expectations
- Meet Staff Needs
- Deliver the Projects and Services On time/Under Budget
- Do it Now & Get it Done Yesterday!



13

## Cyber Security Strategy

- Data & Network Security
- Virus & Malware Protection
- Managing Mobile Devices
- Maintaining Secure Configurations



14

## Cyber Security Strategy

- Managing User Privileges
- Website Filtering & Protection
- Risk Management

*100% Supported by CEO & Commission!*



15

## Management Support!

- Communicate Cyber Risk to Management
- Educate Employees on Cyber Security
- IT Professionals Understand the Risk
- Manage Risk




16



### Cyber Attack Trends

Ransomware malware is a growing concern

The greatest cybersecurity threats are posed by C-level executives





Water Environment Federation  
the water quality people

17

As technology improves, people are the low hanging fruit.

Social engineering takes advantage of the human weakness





Water Environment Federation  
the water quality people

18

## Email Security Guidelines

1. Use strong passwords that are unique
2. Watch out for phishing emails
3. Never open unexpected attachments
4. Verify the email address
5. Verify email request via telephone



19

## Spartanburg Water Case Study: Mobile Devices Multiply!

Data at our Fingertips !

- Expand Mobile Devices to Field Services
- Utilize Mobile Work Order Systems to Communicate
- Utilize GIS in the Field for our Staff



20

## Results?

- < 5 years Mobile Devices - Tablets and Smart Phones Expand from a handful to 165 units used daily by Field Personnel.
- Field Personnel have devices assigned to them

*30% of our Entire Workforce Deployed*



21

## Mobile Device Management Plan

- Users are required to have passwords on smart phones
- Operating system updates are managed and applied
- Allows devices to be located if misplaced



22

## Summary

- Top Down Support and Funding.
- Incorporate Cyber Security Strategy for your utility. Review Regularly!
- Understand the risks areas for your utility. Review Regularly!
- Train Staff. Test. Train the Staff. Test.

23

## Our Next Speaker:



**Elkin Hernandez**  
*Maintenance Director*

- Power and I&C.
- 20+ years of experience of design, construction, commissioning, maintenance and operation of water and power utilities.
- Chair of WEF IWT committee

*DC Water*



24

## Practical approach to Cybersecurity for Industrial Control System (ICS)



25

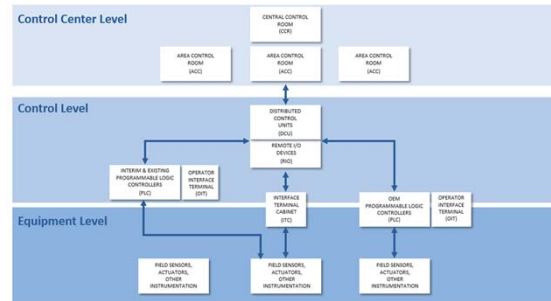
### DC Water At A Glance

- DC Water provides more than **681,000 residents** and **21.3 million annual visitors** in the District of Columbia with retail water and wastewater (sewer) service. With a total service area of approximately **725 square miles**, DC Water also treats wastewater for approximately **1.6 million people** in neighboring jurisdictions, including Montgomery and Prince George's counties in Maryland and Fairfax and Loudoun counties in Virginia.



26

# Background



Industrial control system (ICS) is a general term that encompasses several types of control systems and associated instrumentation used for industrial process control. These systems receive data from remote sensors for monitoring and control purposes. The larger systems are usually implemented by Supervisory Control and Data Acquisition (SCADA) systems, or distributed control systems (DCS), and programmable logic controllers (PLCs), though SCADA and PLC systems are scalable down to small systems with few control loops.

# Security?

*It is all about Availability (and Reliability)*

80's PLCs become popular Proprietary networks

Late 90's Control systems start to move to IP based networks

Early 2000's first Windows based systems

Virus? Just keep it isolated from the internet (air gap), nothing will happen!!

## The new Reality

*Needs:*  
update systems  
share information



*Virus are spread !*

*Now I need an up-to-date AV, this is getting complicated!*

29

## The new Reality

*STUXNET*

Worn

PLCs

Windows



30

## Things to Consider (1)

### *Process Assessment:*

*Policies & Procedures*

### *Logical Access:*

*Provisioning of access*

*Periodic User access review*

### *Change Management*

*System development life cycle*

*Testing*

*Segregation of activities*

### *Recoverability*

*Backup management*

*Backup and recovery controls*



31

## Things to Consider (2)

### *Network Architecture*

*Security Architecture*

*Device configuration*

### *Network Security*

*Identify weaknesses on the design that may allow an internal attacker to compromise the availability, confidentiality and availability of the network.*

### *Vulnerability Assessment*

*Identify common vulnerabilities*



32



## The people



IT or Process Control?

There is a place for everyone

Leverage skills sets

Learning Curve

O&M impact



33

## Good Practices

Audits - DHS

Training - Sans, ISA

Emergency Response (What if?) - Drills

Resources

- The Water Information Sharing and Analysis Center (WaterISAC)
- <https://www.us-cert.gov/ics>
- <https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance>
- <https://www.nist.gov/cyberframework>



34



For further information, contact:

Elkin Hernandez      [Elkin.Hernandez@dcwater.com](mailto:Elkin.Hernandez@dcwater.com)



35

## Our Next Speaker:



**John H. Sudduth**  
*Director of Information  
Technology*

- 25 Year IT professional
- Currently holds several IT security certifications
- Member ISACA
- Member ISC2

*Metropolitan Water Reclamation  
District of Greater Chicago*



36

# Firsthand Experience with a Cyber-Attack



37

## Agenda

- Purpose
- What Happened
- Recent Public Sector Events
- Lessons Learned
- Must-haves to defend against cyber attacks



38

## Purpose of This Presentation

- Is Not To:
  - Promote tools
  - Promote fear
- Is to:
  - Educate
  - Show Sophistication of Targeted Attacks

## What Happened (the Phishing)

- Spear phishing emails sent to targeted employee email accounts (available on the internet)
- Some employees clicked on a link in the email and provided their username and password
- Employee's username and password were used to gain access to their email by unknown perpetrators via Web Mail.
- Phishing emails were sent from internal employee accounts to other internal employees
- Additional employees clicked on the email as it was from a trusted internal employee

## What Happened (the complexity)

- Dedicated Web domains created to make phishing email links look legitimate
- Used Agency logo to make survey page look legitimate
- Website certifications acquired to thwart suspected fraudulent website alerts
- Email filters setup on user accounts to prevent communications from IT
- Exploration of employee account access



41

## What Happened (mitigation)

- Report of unauthorized bank account information changes received from User
- Accounts identified as having bank account info changed
- Fraudulent bank routing and account information identified
- Reported activity to authorities
  - Department of Homeland Security (DHS)
  - FBI
  - Chicago Police Department



42

## Recent Public Sector Events

- Hackers breach 20 Texas government agencies in ransomware cyber attack
  - *Reported 8/19, still under investigation*
  - *Shows how perpetrators work together*
- Social Engineering Attack Nets \$1.7M in Government Funds (*Cabarrus County, N.C., paid scammers \$2.5 million*)
  - *Reported 8/14*
  - *Total of ~9 months*
  - *Perpetrators had direct contact with Agency employees*
  - *Perpetrators posed as contractor*



43

## Lessons Learned

- Train Users on Social Engineering
  - Email phishing
  - Cold calls
  - Change management
- Be prepared (not a matter of if...)
  - Incident response plan
  - Cyber insurance
  - Consider internal phishing campaign



44

## Must-haves to defend against cyber attacks

- **End user training**
- Incident response plan
- Vulnerability assessments
  - Internal phishing
  - Penetration testing
- Adequate funding

*"The best defense is a good offense"*

## Further Research

- Homeland Security effort:  
<https://www.dhs.gov/topic/cybersecurity>
- AWWA: <https://www.awwa.org/Resources-Tools/Resource-Topics/Risk-Resilience/Cybersecurity-Guidance>
- Water Infrastructure Act of 2018