

Cybersecurity SIMPLE

And how to not
get hacked.

Chris Sosnowski, CEO

Mobile: (Provided during class)

chris@waterly.com



Waterly



“Down and Dirty” Outline

- Background
 - Rural Cybersecurity Background for Water/Wastewater
 - What is the need for this course and courses like it?
 - Instructor Background
- Network Fundamentals for Operators
 - How to Hack People
 - How to Hack Water Cybersecurity Things
- Risks
 - The Cloud
 - You
 - Who is responsible?
- Call to Action
 - Questions to ask Cloud Providers, Integrators, and IT

The background of the slide is a dark, abstract network of glowing lines and nodes in shades of blue, green, and red, creating a sense of digital connectivity and data flow.

The need for Cybersecurity in Rural Water

What we should know to justify paying attention today

The Need for Cybersecurity Awareness in Rural

This email from Fall 2023:



NRWA

RURAL WATER WIRE

U.S. Senators Introduce Bills to Enhance Rural Cybersecurity

Government Technology reports that the Cybersecurity for Rural Water Systems Act and the Food and Agriculture Industry Cybersecurity Support Act would address vulnerabilities in agricultural systems and help farmers and ranchers prevent and respond to cyber threats.



[Read More](#)

<https://www.govtech.com/security/u-s-senators-introduce-bills-to-enhance-rural-cybersecurity>



A recent letter from the White House

THE WHITE HOUSE
WASHINGTON

March 18, 2024

Dear Governor:

Disabling cyberattacks are striking water and wastewater systems throughout the United States. These attacks have the potential to disrupt the critical lifeline of clean and safe drinking water, as well as impose significant costs on affected communities. We are writing to describe the nature of these threats and request your partnership on important actions to secure water systems against the increasing risks from and consequences of these attacks.

Two recent and ongoing threats illustrate the risk that cyberattacks pose to the nation's water systems:



More Bad News

- When we got into water, one of the reasons was because we **don't** like technology
- You *probably* don't know what you're talking about
- You *likely* have (very) limited funding
- You *almost certainly* have inadequately trained staff (who is adequately trained on cybersecurity anyhow)
- Sometimes overreacting causes other problems
- Elected officials typically don't understand the risk **AND** expect that nothing will happen
- This is sometimes considered scary stuff...**but not as much after today!**

Recap of the Need for Today's Training

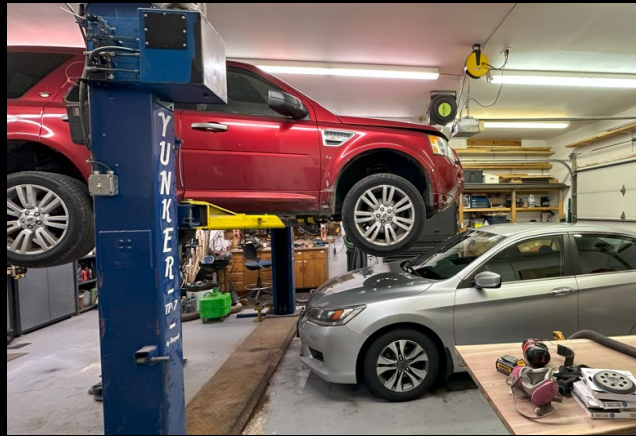
- I've been doing this a long time and seen a lot of stuff
- Cybersecurity incidents DO HAPPEN
- Bad things happen to good people
- Small utilities are "hacked on" every day in the US
- Spending money & hiring consultants won't solve the problem alone

GOOD NEWS: The answer starts with you...today.



Who am I?

Instructor Background



Chris's Background

- 20 Years in SCADA and Cyber Consulting & Integration
- Authored / Co-Authored over 50+ government SCADA design plans that cover over 5 million people
- Volunteer Educator for water and wastewater for 20+ years
- Gear Head / Water & IT Nerd
- I run a software company in my spare time. ;-)

I can speak English, SCADA, Water, IT and Cybersecurity

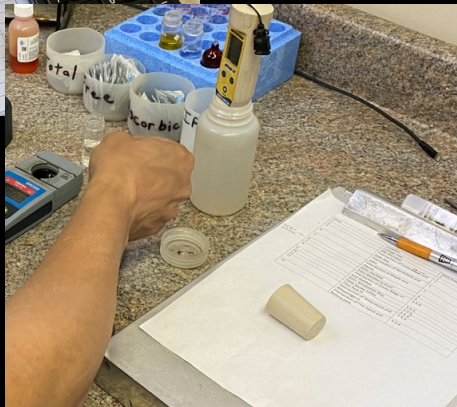
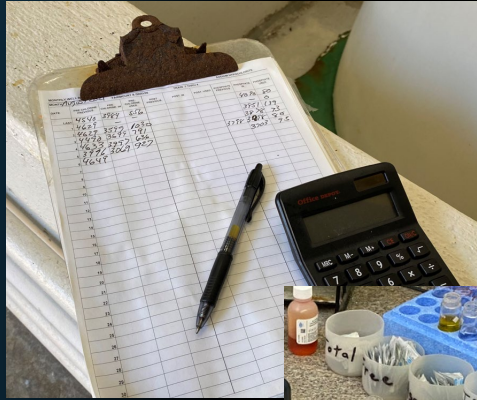


Waterly

Helping water & wastewater implement an **easy-to-use**, standardized plant asset and data management in days, not months, ...more affordably than anyone.

What is Waterly? AND GET YOU TO DIGITAL, SECURE, & SIMPLE

WE TAKE THIS RURAL AMERICAN MADNESS



Fairmont & Garvin (WTP) BLDG A - City of Joliet Utilities (L1970450) MOR
 May 2022
 ILLINOIS ENVIRONMENTAL PROTECTION AGENCY - DIVISION OF PUBLIC WATER SUPPLIES

DATE	T1-H40 Day Tank		T1-H40 Day Tank		T1-101 Meter		T1-101 Meter		T1-101 Meter		T1-101 Meter		T1-101 Meter		T1-101 Meter		T1-101 Meter		T1-101 Meter		REMARK
	H40 Used (MG)	Calc'd H40 (MG)	H40 Used (MG)	Calc'd H40 (MG)	Flow (MGD)	Flow (MGD)	H40 Used (MG)	Calc'd H40 (MG)	Flow (MGD)	Flow (MGD)	H40 Used (MG)	Calc'd H40 (MG)	Flow (MGD)	Flow (MGD)	H40 Used (MG)	Calc'd H40 (MG)	Flow (MGD)	Flow (MGD)	H40 Used (MG)	Calc'd H40 (MG)	
1	872	1.18	316	0.66	887	577	68	0.11	606	0.82	711	597	1,643	7.45	126	0.82	-	-	2.28	-	-
2	262	0.69	1,038	2.05	457	608	232	0.58	1,606	2.80	477	603	764	5.19	64	0.54	-	-	2.14	-	-
3	326	0.67	819	1.69	840	580	124	0.23	0	0.00	657	579	567	4.11	68	0.58	-	-	2.21	-	-
4	1,092	1.96	140	0.22	369	514	688	2.48	710	1.51	414	565	1,216	6.98	55	0.47	2.50	2.52	2.80	2.80	0.02
5	496	0.69	850	1.48	867	665	344	0.62	64	0.14	663	554	497	2.58	44	0.29	-	-	2.12	2.80	-
6	1,182	2.61	132	0.22	399	608	724	2.23	314	1.16	900	530	1,213	9.29	63	0.60	-	-	2.14	-	-
7	316	0.48	622	1.33	786	562	144	0.29	0	0.00	605	528	407	2.34	37	0.27	-	-	2.26	-	-
8	0	0.00	16	0.02	991	850	678	0.78	662	0.99	1,041	867	-	-	-	-	-	-	2.05	-	-
9	1,260	2.93	588	0.74	515	595	966	3.33	1,034	1.95	355	635	927	5.50	102	0.74	1.80	1.71	1.90	2.10	2.00
10	0	0.00	0	0.00	697	1,286	310	0.65	1,220	1.34	830	1,014	738	2.81	42	0.19	-	-	1.71	2.00	-
11	0	0.00	612	0.82	573	500	1,228	2.94	364	0.43	500	1,005	877	4.27	83	0.50	-	-	1.69	-	-
12	0	0.00	204	0.31	570	793	220	0.34	1,446	3.27	774	530	503	2.70	-	-	-	-	2.40	-	-
13	334	0.54	64	0.17	740	437	1,316	2.41	396	0.61	655	1,170	1,513	7.93	85	0.51	2.10	1.78	2.30	2.30	-
14	-	-	-	-	731	1,041	-	-	-	-	1,004	564	-	-	-	-	-	-	1.59	-	-
15	984	1.91	420	1.09	738	484	880	1.42	1,014	1.12	677	1,084	1,697	8.37	132	0.80	2.10	1.73	2.20	2.00	-
16	236	0.37	196	0.24	740	995	462	0.54	1,440	3.09	1,004	959	547	2.88	40	0.25	-	-	1.63	-	-
17	1,112	2.62	446	1.71	508	313	942	2.48	334	0.39	456	1,033	1,299	8.23	56	0.44	2.80	1.95	2.80	3.00	-
18	136	0.39	196	0.33	510	720	204	0.35	444	2.05	706	389	389	3.38	14	0.26	2.20	2.30	2.30	2.30	-
19	1,390	3.12	766	2.97	519	309	1,006	2.65	336	0.48	456	838	1,174	8.09	57	0.48	2.60	2.18	2.50	2.70	-
20	152	0.33	256	0.37	559	835	404	0.61	414	1.18	796	422	364	1.98	25	0.17	-	-	2.02	-	-
21	-	-	-	-	662	0	-	-	-	-	656	976	-	-	-	-	-	-	2.03	-	-
22	906	1.57	438	1.27	691	414	404	0.75	1,040	1.33	646	936	1,636	8.77	110	0.74	-	-	2.22	2.80	-
23	1,146	1.00	88	0.13	468	637	662	0.88	666	3.09	729	716	1,113	56	0.50	-	-	2.40	2.60	0.03	-
24	253	0.43	648	1.38	698	365	264	0.44	0	0.00	722	532	455	3.58	37	0.26	-	-	2.35	2.50	-
25	1,162	2.97	0	0.00	469	620	582	2.24	314	1.13	311	546	443	3.31	51	0.47	2.10	1.85	2.80	2.10	0.02
26	354	0.56	744	1.55	755	575	406	0.64	70	0.15	768	657	644	5.00	39	0.27	2.08	2.60	2.60	0.01	-
27	940	2.43	0	0.00	464	612	524	2.03	430	0.56	310	536	421	3.19	58	0.54	-	-	2.04	-	-
28	588	1.32	458	0.66	533	838	174	0.41	740	1.39	716	532	-	-	-	-	-	2.04	-	-	-
29	316	0.48	622	1.33	786	562	144	0.29	0	0.00	605	528	407	2.34	37	0.27	-	-	2.26	-	-
30	274	0.48	1,225	2.06	665	516	268	0.45	0	0.00	714	527	544	2.95	43	0.29	-	-	1.95	2.80	-
Total	15,023	3.61	11,205	2.97	16,591	26,484	14,354	16,814	16,976	20,927	25,932	3,399	1,735	-	-	-	-	-	-	-	-
Max	1,390	3.12	766	2.97	991	1,286	1,316	3.33	1,440	3.27	1,041	1,170	2,019	9.29	141	0.83	2.80	2.35	2.80	3.00	2.80
Min	0	0.00	0	0.00	399	0	68	0.11	0	0.00	309	383	364	1.98	25	0.17	1.80	1.59	1.90	2.00	
Avg	379	1.31	415	0.87	632	639	508	1.27	546	1.87	615	676	885	5.02	67	0.47	2.27	1.98	2.42	2.41	

Click to visit Waterly's Website

The screenshot displays the Waterly web application interface. On the left is a navigation sidebar with a 'Dashboard' button selected. The main content area is divided into two sections. The top section, 'Historical Metrics', shows a line graph for 'System Summary - System Wide - Total Flow (MGD)' from 12/1/2020 to 1/17/2023. Below the graph is a table of metrics:

Metric	Min	Arg	Max	Sum	Unit
System Summary - System Wide - Angle Tam Flow (MGD)	0.018	0.535	0.973	398,952	MGD
System Summary - System Wide - Randall Flow (MGD)	0.05	0.249	0.583	185,888	MGD
System Summary - System Wide - Total Flow (MGD)	0.47	0.784	1.224	584,84	MGD

The bottom section, '3D Facility Viewer', shows a virtual 3D model of a water treatment plant facility with various equipment like pumps and valves labeled.

Excel ribbon: File, Home, Insert, Reference, Layout, Formulas, Data, Review, View, Developer, Help

Table: FOUNTAIN HILLS SANITARY DISTRICT MONTHLY GENERATOR REPORT. Columns: MONTH, YEAR, DAILY RUN TIME (HRS), EXERCISE, LOAD, INSPECTION DWM, REMARKS.

Table: Fountain Hills Sanitary District ASR-1, ASR-2, ASR-3, ASR-4. Columns: Month, Injected, Wasted, Recovered, AC-FT, WASTED, RECOVERED.

Table: Fountain Hills Sanitary District Desert Vista Park Meter Reads. Columns: Date, Meter Reading, Gallons Used, Comments.

Table: Fountain Hills Sanitary District Eagle Mountain Meter Reads. Columns: Date, Meter Reading, Gallons Used, Comments.

Table: ASR Well Daily Summary. Columns: Date, Total Injected.

We help you ditch the:

Spreadsheet Madness!!

Table: Monthly Process Control. Columns: WEATHER, WWTP FLOW, AWT FLOW, INFLUENT, WEST A.

Table: Fountain Hills Sanitary District Daily Meter Reads, September 2021. Columns: Meter ID, Location, Meter Reading, Gallons Used, Comments.

Table: ASR Well Daily Summary (continued). Columns: Date, Total Injected.

Table: ASR Well Daily Summary (continued). Columns: Date, Total Injected.

Table: Fountain Hills Sanitary District Daily Meter Reads, September 2021 Meter Locations and Units. Columns: Meter ID, Location, Meter Reading, Gallons Used, Comments.

Table: Fountain Hills Sanitary District Daily Meter Reads, September 2021 Meter Locations and Units (continued).

Table: ASR Well Daily Summary (continued). Columns: Date, Total Injected.

And Ditch the Clipboard



And get smart, clean data:

West Dundee, IL

Dashboard

Reporting

MY SITES +

- System Summary
- Non-Revenue Water
- Sampling
- Chlorine Residuals
- Angle Tarn WTP
- Angle Tarn - Supervi...
- High to Mid zone PR...
- FRWRD Flume
- Jelke LS
- 3rd St LS
- Well #1
- Liberty LS
- 5th St Booster Stati...
- Kittridge BS
- Grand Pointe LS
- Carrington LS
- Timbers & Valley LS
- Rt 72 GS
- Oakview LS
- Randall Road WTP
- Randall Road - Supe...
- Elm Ct Flume
- Locust Flume

Historical Metrics

< 12/1/2020 - 1/17/2023 >

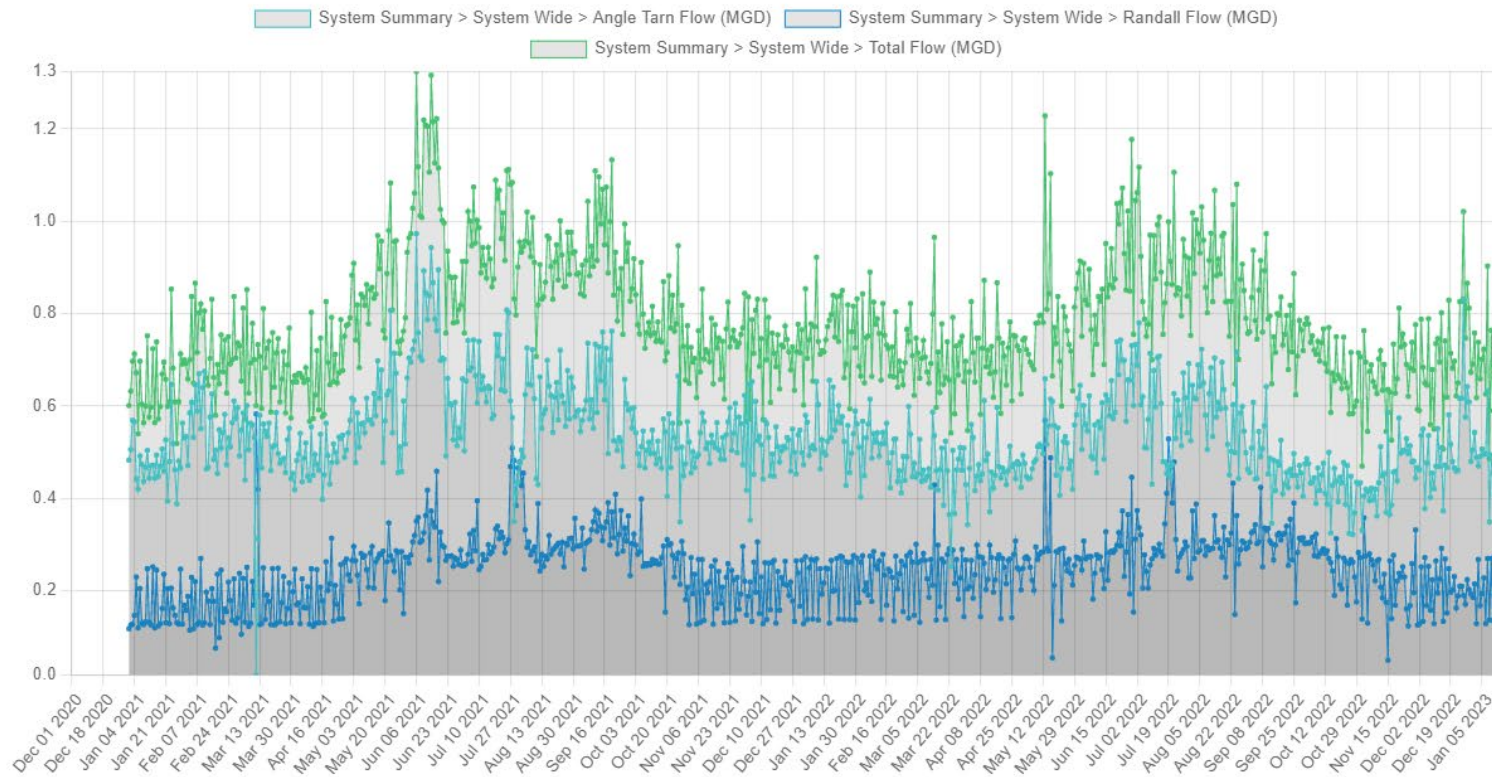


No Saved Trends

EDIT SAVED TRENDS

Select Metrics

- System Summary > System Wide > Angle Tarn Flow (MGD) x
- System Summary > System Wide > Randall Flow (MGD) x
- System Summary > System Wide > Total Flow (MGD) x



Metric	Min	Avg	Max	Sum	Unit
System Summary > System Wide > Angle Tarn Flow (MGD)	0.018	0.535	0.973	398.952	MGD

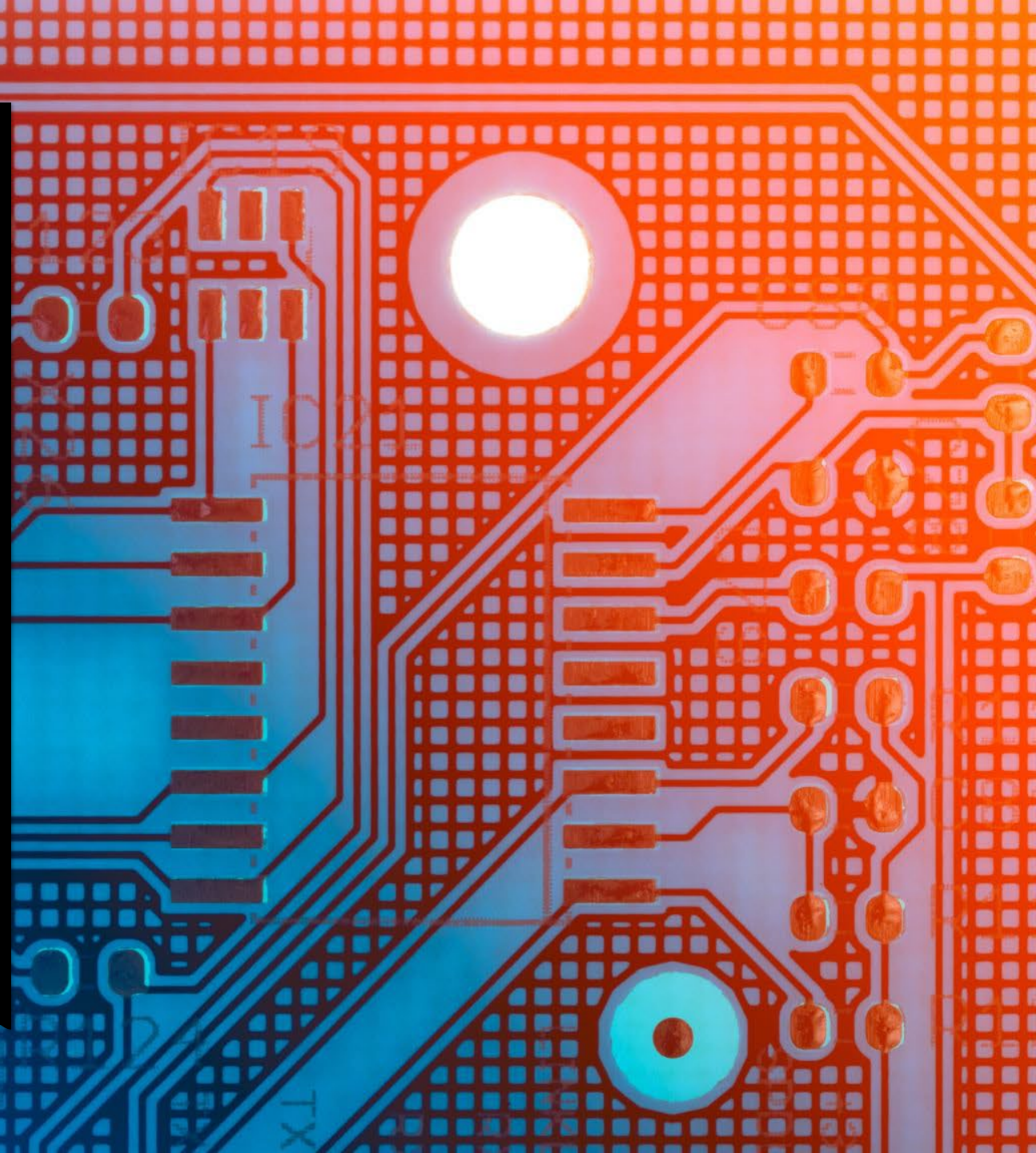


Network Fundamentals for Operators & Clerks

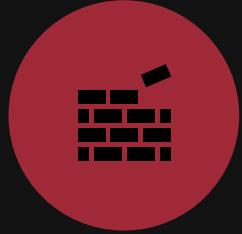
Don't worry...we won't geek out too much

The “ZONES”

- Information Technology (IT) Network
- Operational Technology (OT) Network
- Demilitarized Zone (DMZ)
- The (Public) Internet



Usual Things in your Network Zones



FIREWALL – SEPARATES NETWORKS WITH SPECIFIC, DETAILED, TRAFFIC RULES



ROUTER – SEPARATES NETWORKS AND DIRECTS TRAFFIC



VPN – SECURED & ENCRYPTED REMOTE ACCESS

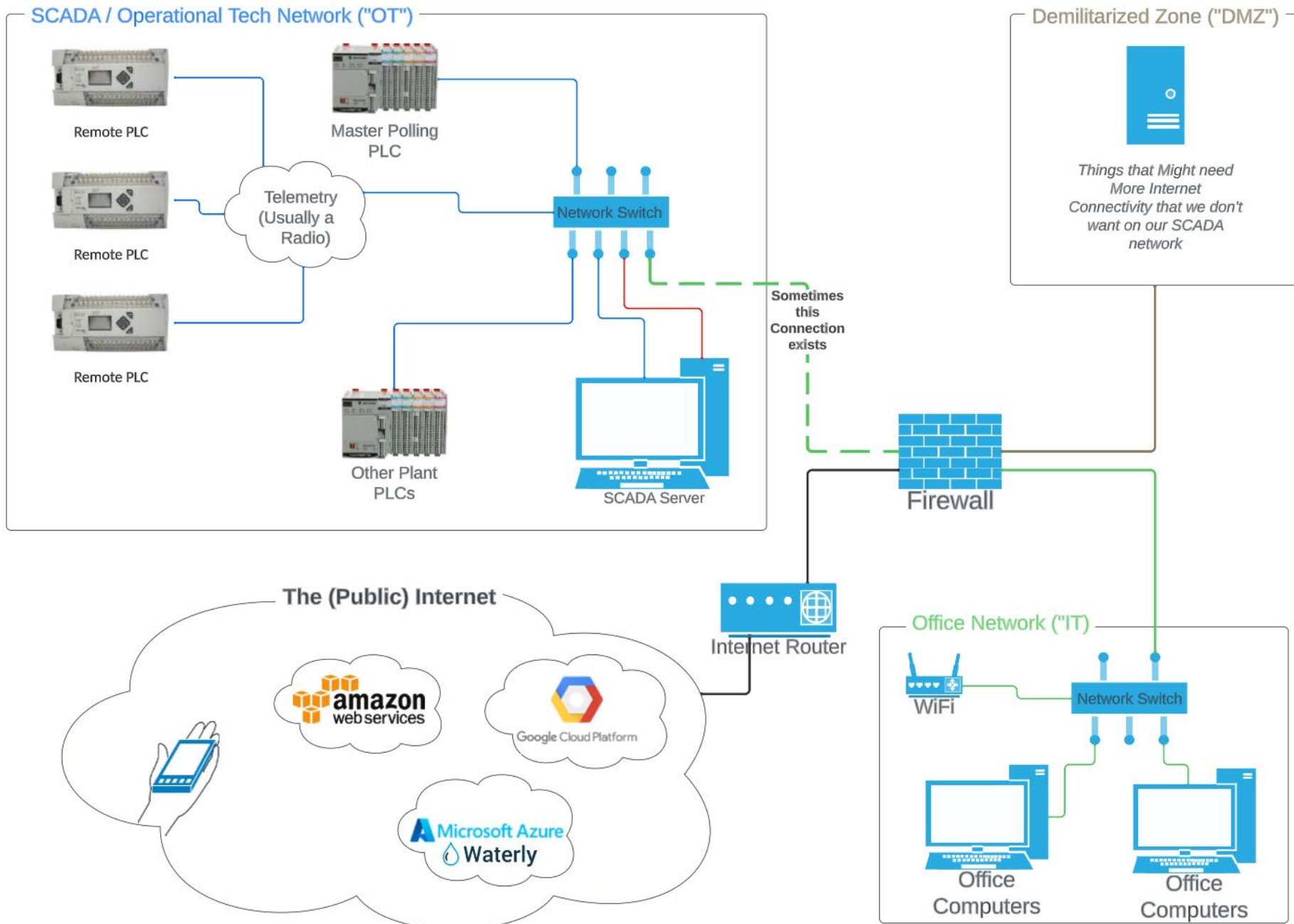


SCADA – YOUR PROBABLE LARGEST RISK...BUT NOT IN THE WAY YOU THINK.














THE CLOUD – ANOTHER PROBABLE LARGE RISK

Water Network Components - for Operators



Cloud Tools for managing Water Data

Tool	Readiness	Notes
Email		Already done in most every case.
Spreadsheets, documents		Office 365 and Google Docs!
GIS		Plenty of Options here. Start small and simple.
AMI/AMR		Plenty of Cellular, Fixed, and Satellite Options.
Reports		So much better than Excel. MORs? Sewer (defect) videos? Leak detection?
Sensors (“IoT / IIoT”)		Limited options for rural. Ask lots of questions before buying!
Historians		Start collecting data now that future generations will appreciate
SCADA Alarming		Probably not so much for critical alarms
SCADA Viewing		More couch time...less driving, quicker response to critical issues.
<u>SCADA</u> Control		LOCAL CONTROL IS REQUIRED - backup Internet & SLA must be considered
<i>Supervisory</i> Control		Lift Stations, booster pumps, water towers, setpoint changes. Know the right Cybersecurity questions to ask.

A hooded figure, likely a hacker, is seen from behind, sitting at a desk with a laptop. The background is a dark cityscape at night, with many skyscrapers and lights. A complex network of glowing blue and orange lines is overlaid on the scene, suggesting a digital or cyber environment. The text "What do hackers understand?" is centered in the image in a large, white, sans-serif font.

What do hackers understand?

They understand hacking **people AND** hacking **technology**

The background features a complex, abstract network of glowing lines in shades of blue, teal, and red, forming a mesh-like structure that recedes into the distance. The lines are interconnected, creating a sense of depth and connectivity.

Hacking People

Passwords and Phishing

Crowd Participation

The results were that 60% of the audience had their personal email compromised and about 20% of the room had their work emails compromised!

10%+ of this room has been hacked in the last 3 years and doesn't know it

...let's see if I'm right.

[HAVEIBEENPWNED.COM](https://www.haveibeenpwned.com)



Phishing and Social Attacks

Purchase Successful!

Dear,

Your 12 months maintenance support charged for NORTON Antivirus Defender firewall has been debited successfully.
Your account has been charged for an amount of \$499.99.
This email is sent for notification purpose,
If you have any concern about it please contact our customer support at [+1 \(800\) 229-1748](tel:+18002291748)

Order Details:

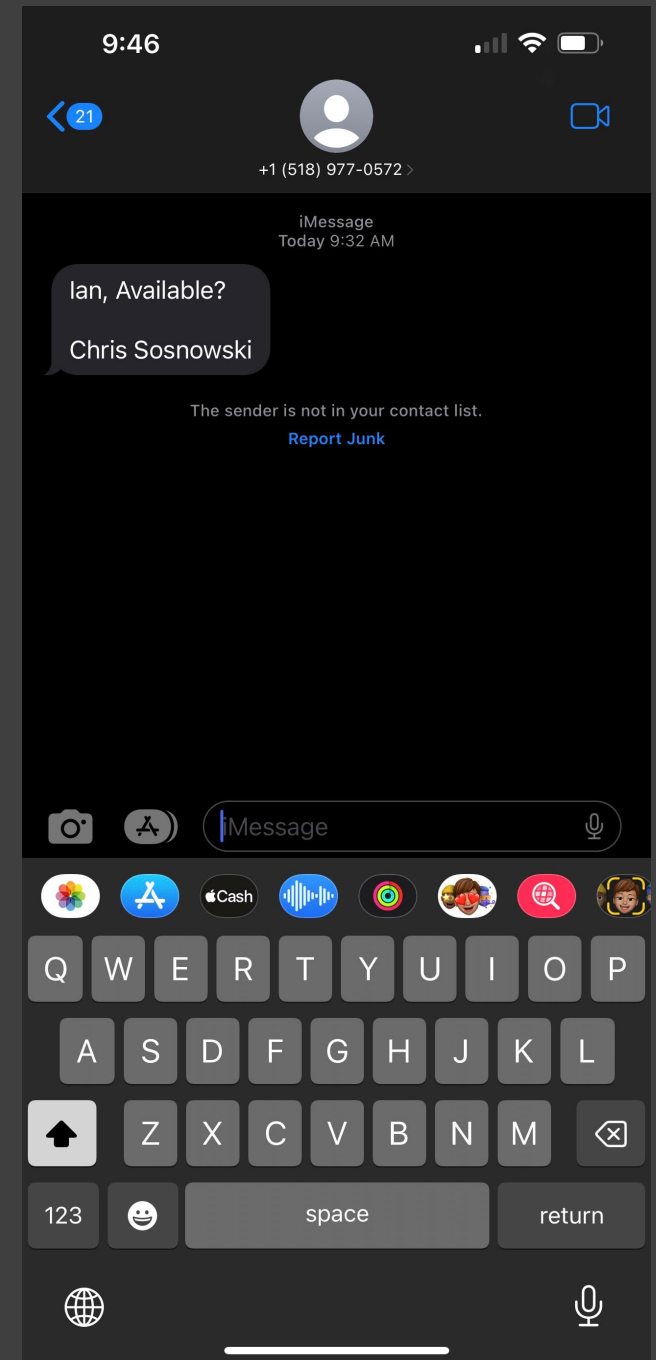
Product:	*NORTON ANTIVIRUS
Date:	09/27/2021
Total Amount Including All Taxes:	\$499.99
Order Id:	NHJU-0987-456
Payment Method:	Auto Debit

Have questions? Contact our team immediately
Helpline:

+1 (800) 229-1748

Thanks for Purchase!!

***NORTON Team!**



Protect Yourself from Phishing

1. Read the **WHOLE** message and think about it
2. Keep your computer and devices updated by enabling “auto-update” features.
3. Use multi-factor authentication

Protect your Identity

- Know thyself – what is identity management?
- How do we know you are really you? (there are 3 ways)
- Why do passwords need to be so stupid and complicated?
- Is there anything to help us with the madness?

YES!

Get yourself some Password Management
Tools: 1Password, LastPass & Dashlane

The background features a complex, abstract network of glowing lines in shades of blue, teal, and red, forming a mesh-like structure that recedes into the distance. The lines are interconnected, creating a sense of depth and connectivity.

Hacking Technology

It's easier than you think...but not as easy as people?

Some quick (legal) fun (if we have time)



Shodan Maps Images Monitor Developer More...

SHODAN Explore Downloads Pricing [city:milwaukee product:rockwell](#) 🔍

TOTAL RESULTS

2

TOP ORGANIZATIONS

Cellco Partnership DBA Verizon Wireless	1
Charter Communications Inc	1

TOP VERSIONS

1756-ENBT/A	1
1766-L32BXB B/15.00	1

[View Report](#) [Download Results](#) [Historical Trend](#) [View on Map](#)

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

65.30.0

rrcs-65-30-0-central.biz.rr.com
[Charter Communications Inc](#)
United States, Milwaukee

ics

Product name: 1766-L32BXB B/15.00
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x40650ca4
Device type: Programmable Logic Controller
Device IP: 65.30.0

63.45.1

host215.sub-63-1-myvzw.com
[Cellco Partnership DBA Verizon Wireless](#)
United States, Milwaukee

ics

Product name: 1756-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x007f6009
Device type: Communications Adapter
Device IP: 192.168.0.40

The background of the image is a dark blue grid with a pattern of light blue and white hexadecimal characters (0-9, A-F) scattered across it, creating a digital or data-like aesthetic.

A Call to Action

“What do I do tomorrow?”

Who is responsible for Water Cyber security?

- What happens if SCADA is hacked (bad)?
 - Boil order?
 - Sewage backup?
 - Sanitary Sewer Overflow?
- Who is responsible for the reliability (and related risk) of SCADA then?
 - IT
 - The Clerk
 - The Mayor
 - Public Works and the IT Provider
 - Public Works ...or Village/City Management

Calls to Action

- Learn How to Talk about “IT” (and “OT”, right?)
- Passwords
 - Stop using the same password!
 - Get a password manager & learn to use it (maybe another class?)
 - Use Single Sign On (SSO)
- Access NRWA/RWA Funding Sources for Cyber improvements 😊

Ask Good Questions and KEEP LEARNING!

Your Questions?



Chris Sosnowski
chris@waterly.com

