SMALL SYSTEMS AREN'T SMALL POTATOES

WHY RURAL WATER UTILITIES NEED CYBERSECURITY AND WHAT TO DO ABOUT IT, PART 1

PRESENTERS

STEVE MUSTARD
Licensed Professional Engineer and industrial cybersecurity SME. MCGA Board Member and past president of the International Society of Automation (ISA).

JENNIFER LYN WALKER
Director of Infrastructure Cyber Defense, WaterISAC. Cybersecurity professional with over 20 years' experience supporting SLTT and other critical infrastructure sectors.

ANDREW HILDICK-SMITH
Advisor at WaterISAC. Licensed Professional Engineer with 30 years at a water and wastewater utility with responsibilities for SCADA security and emergency planning.

Mission Critical Global Alliance

NRWA

WATER ISAC

CYBERSECURITY AWARENESS

STEVE MUSTARD, MCGA BOARD MEMBER AND FORMER ISA PRESIDENT

WHY ARE WE HERE?

Hack attack causes 'massive damage'

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 3:58 PM EDT

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

LISTEN TO ARTICLE
▶ 4:58

SHARE THIS ARTICLE
Share
Tweet
Post
Email

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack.

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm Mandiant, part of FireEye Inc., in an interview. The account was no longer in use at the time of the attack but

LIVE ON BLOOMBERG
Watch Live TV >
Listen to Live Radio >

Most Read

TECHNOLOGY
Gangrene, Hearing Loss Show Delta Variant May Be More Severe

BUSINESS
There's a New Vision for Crypto, and It's Wildly Different From Bitcoin

BUSINESS
Activist Investor Wants Heads to Roll After $6.2 Billion Cyberpunk Fiasco

A former civil servant of the city of Lopik, working as manager of the sewage system, was fired in 2016 for integrity violations. Several months later, pumps in the sewage system were started and stopped, and valves opened and closed, a wrong combination of which could have caused a spill of sewage, damaged pumps or valves, or broken sewer pipes (luckily this didn't occur). Also, he deleted some 8000 files, which made that remote control of the sewage system was not possible for three days.

BBC Sign in Home News Sport Reel Worklife Travel

NEWS

Home Coronavirus Video World US & Canada UK Business Tech Science Stories Entertainment & A

US & Canada

JBS: FBI says Russia-linked group hacked meat supplier

5 days ago

JBS, founded in Brazil in 1953, is the world's largest meat supplier

A Russian cyber-criminal group was behind a ransomware attack that has targeted the world's largest meat processing company, the FBI has said.

son Oldsmar's
ack, sheriff says

tacker tried to raise levels of
y a factor of more than 100.

s man tampered with
ystem

mpering malware
ical infrastructure

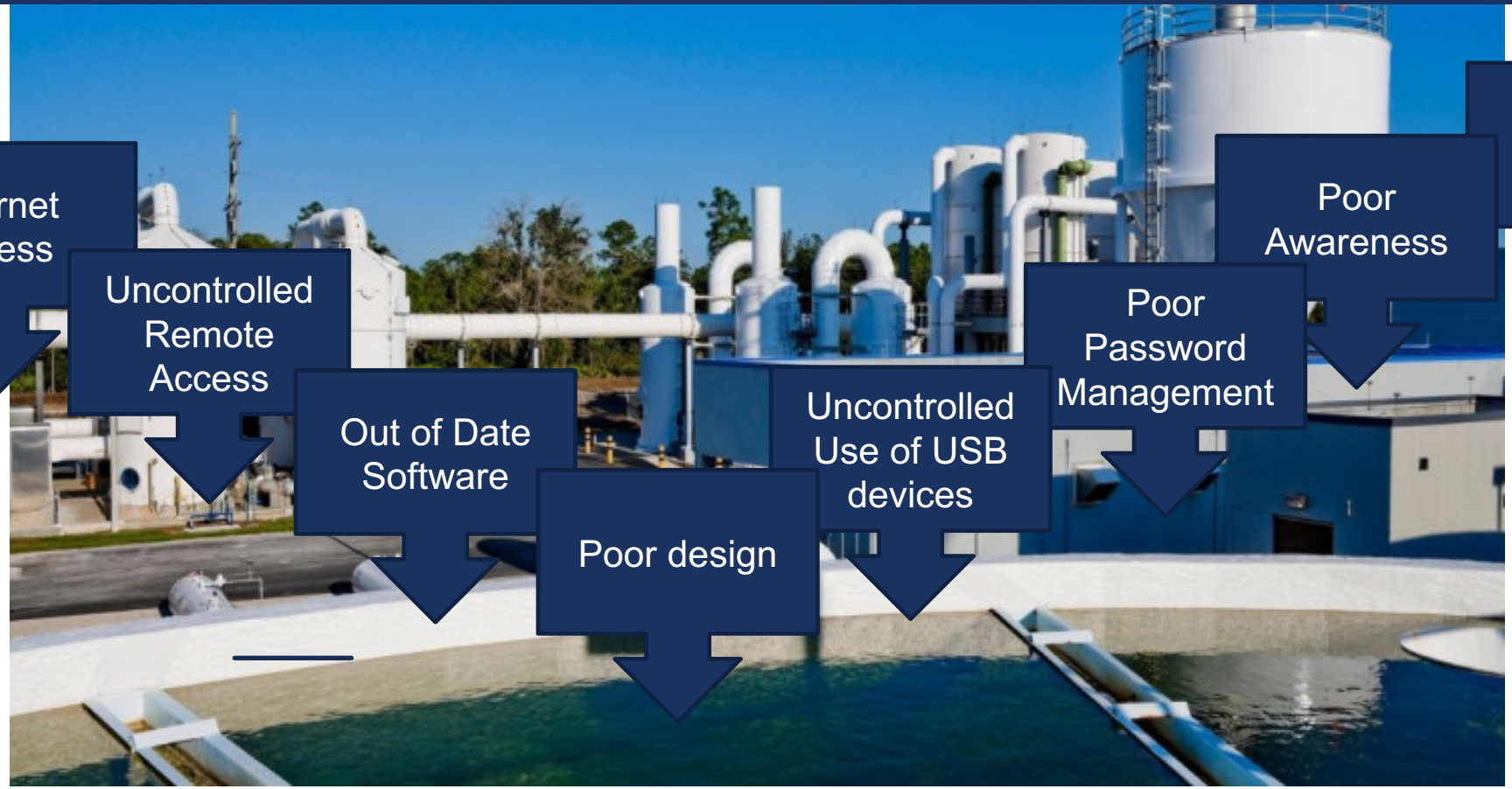
et safety systems isn't an isolated incident.

Mission Critical Global Alliance

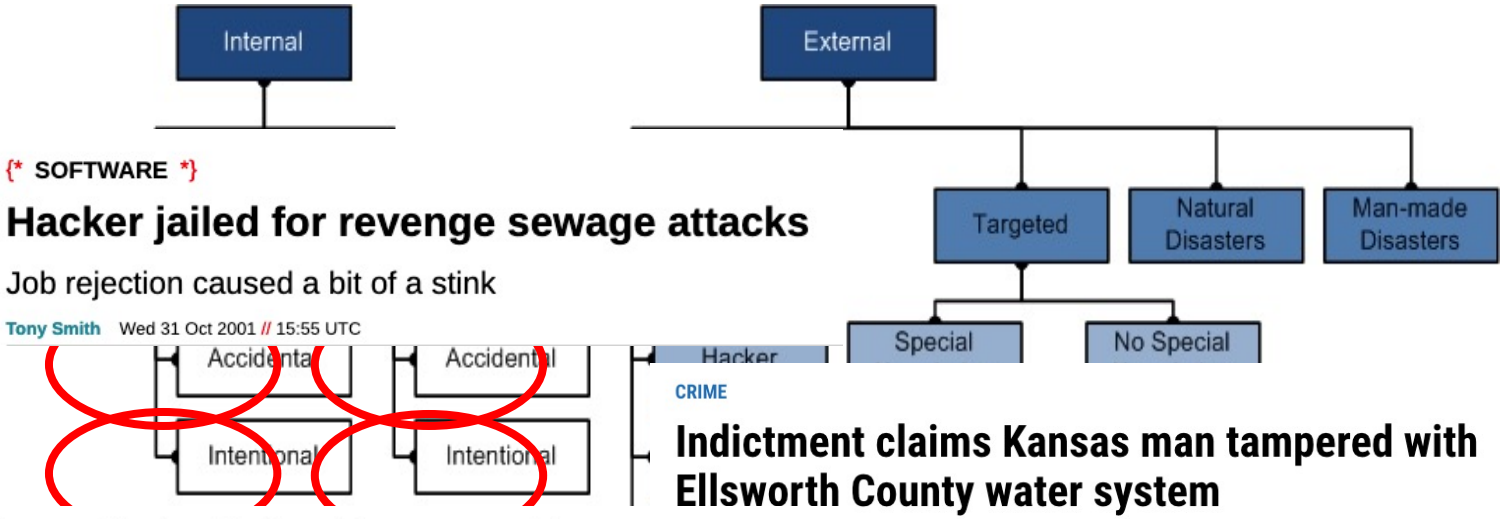
NRWA

WATER ISAC

VULNERABILITIES



POTENTIAL THREAT SOURCES



{* SOFTWARE *}

Hacker jailed for revenge sewage attacks

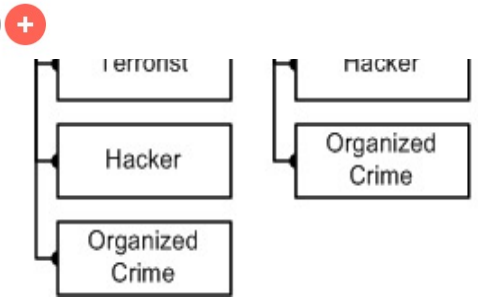
Job rejection caused a bit of a stink

Tony Smith Wed 31 Oct 2001 // 15:55 UTC

A former civil servant of the city of Lopik, working as manager of the sewage system, was fired in 2016 for integrity violations. Several months later, pumps in the sewage system were started and stopped, and valves opened and closed, a wrong combination of which could have caused a spill of sewage, damaged pumps or valves, or broken sewer pipes (luckily this didn't occur). Also, he deleted some 8000 files, which made that remote control of the sewage system was not possible for three days.

CRIME

Indictment claims Kansas man tampered with Ellsworth County water system



Mission Critical Global Alliance

NRWA

WATER ISAC

SOCIAL ENGINEERING

An analysis of more than 55 million emails reveals that one in every 99 emails is a phishing attack.

Even scarier, studies show that 25% of these emails sneak into Office 365, one of the most widely used office suite packages in the world, with over 60 million commercial users. And, the more users a platform has, the higher the chance of phishing attack success.

97% of people cannot identify a phishing scam.

We like to think a robust training program is enough to help employees spot a scam, but phishing attack statistics prove that humans are fallible. While no one is likely to fall for the "Nigerian Prince" scams of yesterday, phishers have become more sophisticated in their techniques so that even the savviest of internet users can become victims.

Office Workers Will Give Away Their Password For A Pen

from the *it's-that-simple* dept
Fri, Apr 18th 2003 3:04pm – Mike Masnick

BBC NEWS

Watch One-Minute World News

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science &

Last Updated: Tuesday, 20 April, 2004, 01:44 GMT 02:44 UK

E-mail this to a friend Printable version

Passwords revealed by sweet deal

More than 70% of people would reveal their computer password in exchange for a bar of chocolate, a survey has found.

It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed.

A second survey found that

Security crumbles in the face of sweet bribes

Mission Critical Global Alliance

NRWA

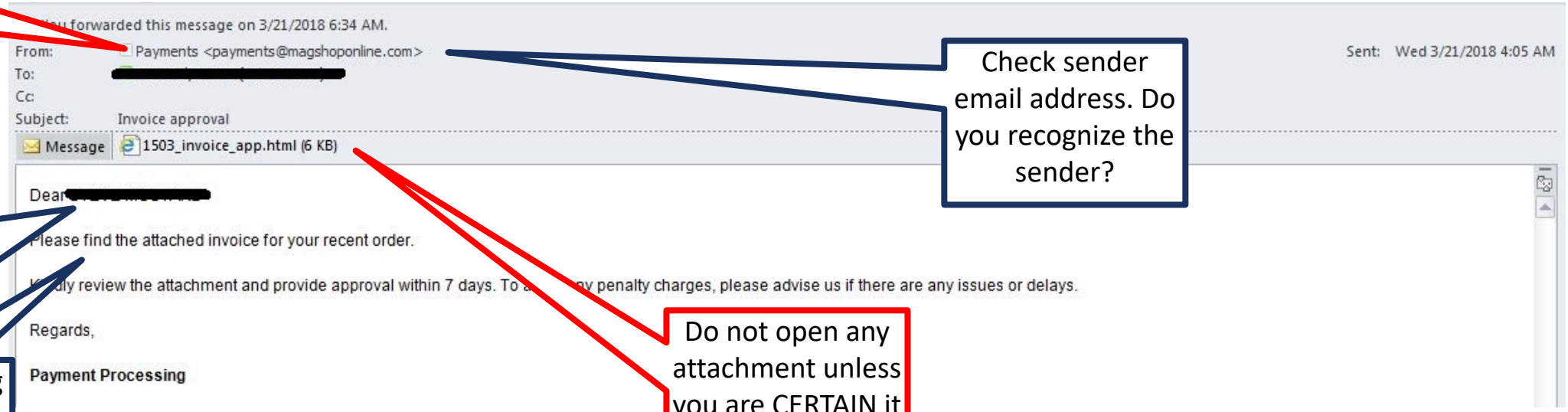
WATER ISAC

WHAT TO LOOK FOR

Do not reply to the sender

Just because they use your name, doesn't mean it can be trusted

Are you expecting an invoice?



Check sender email address. Do you recognize the sender?

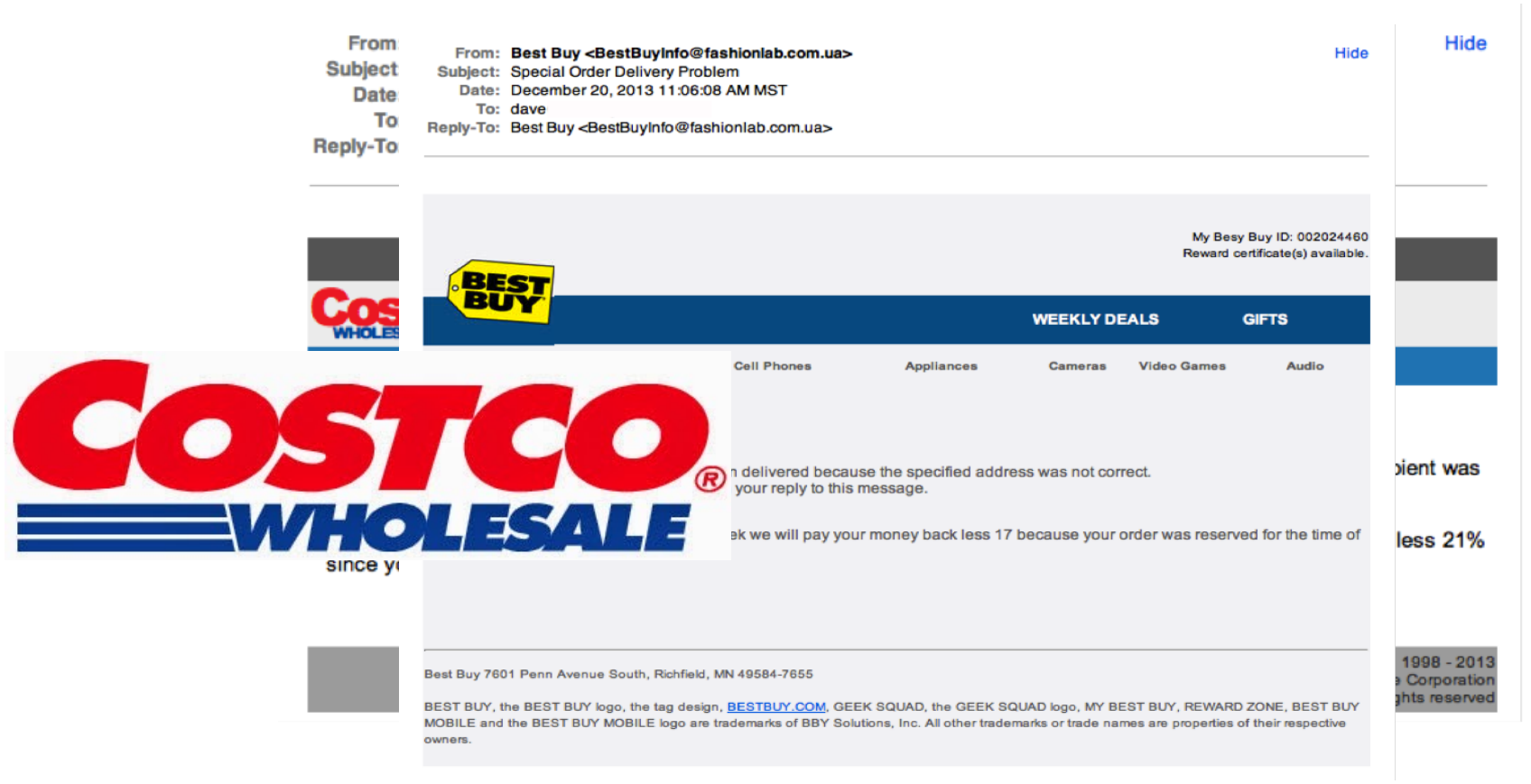
Do not open any attachment unless you are CERTAIN it can be trusted

Mission Critical Global Alliance

NRWA

WATER ISAC

PHISHING EXAMPLES



Mission Critical Global Alliance

NRWA

WATER ISAC

EXAMPLE (NOVEMBER 2021) - FIN7 MALICIOUS USB

U.S.Department of Heath and Human Services

COVID-19

COVID-19 Pandemic Prevention Program

United States Department of Health and Human Services, The Centers for Disease Control and Prevention (CDC), VaccineFinder had applied new regulations for public places, government agencies, restaurants, hotels and companies.

These rules are required and concerned individuals who had been vaccinated, are about to be vaccinated and who have gone through COVID-19 disease. The instructions have been added and updated according to the official guidelines on the prevention and spread of COVID-19.

To confirm that you received the regulations and apply these instructions, you must be familiar with the regulations provided on the USB flash drive. This is required to avoid additional lockdown measures and possible fines for you and your company.

Using the USB Flash drive, go to the website https://www.hhs.gov and pass the mandatory confirmation procedure that you familiarized and applied all of these instructions.

Sincerely,
Ann C. Agnew,
Executive Secretary,
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201

Executive Secretary,
Department of Health and
Human Services

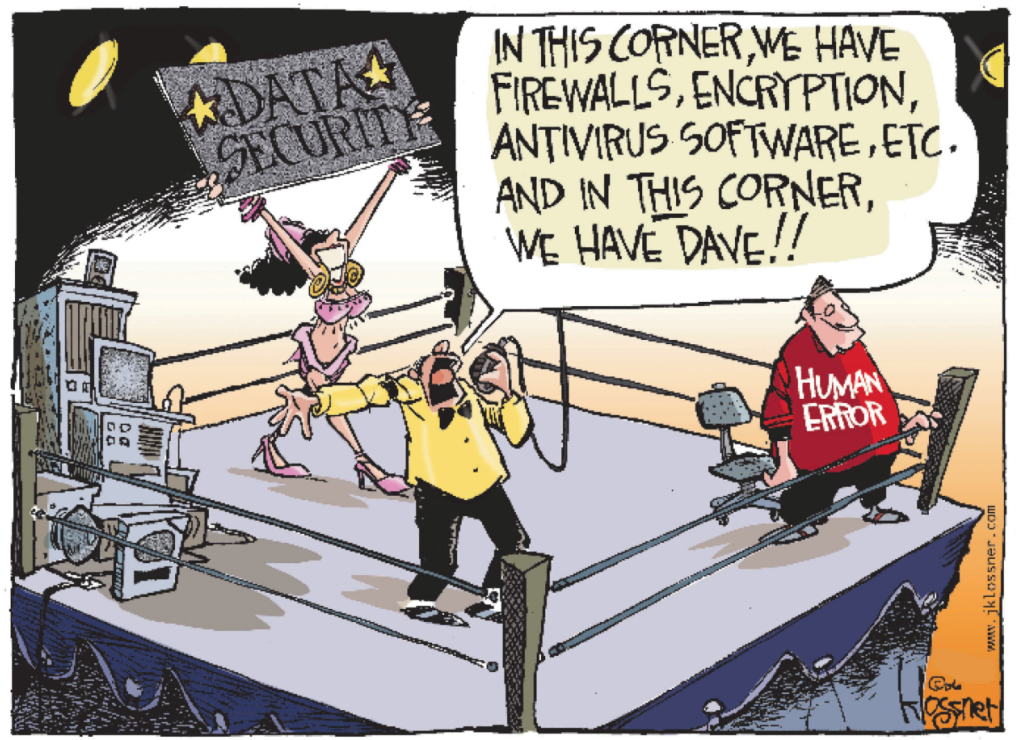
Ann C. Agnew

Mission Critical Global Alliance

NRWA

WATER ISAC

TECHNOLOGY IS NOT INFALLIBLE

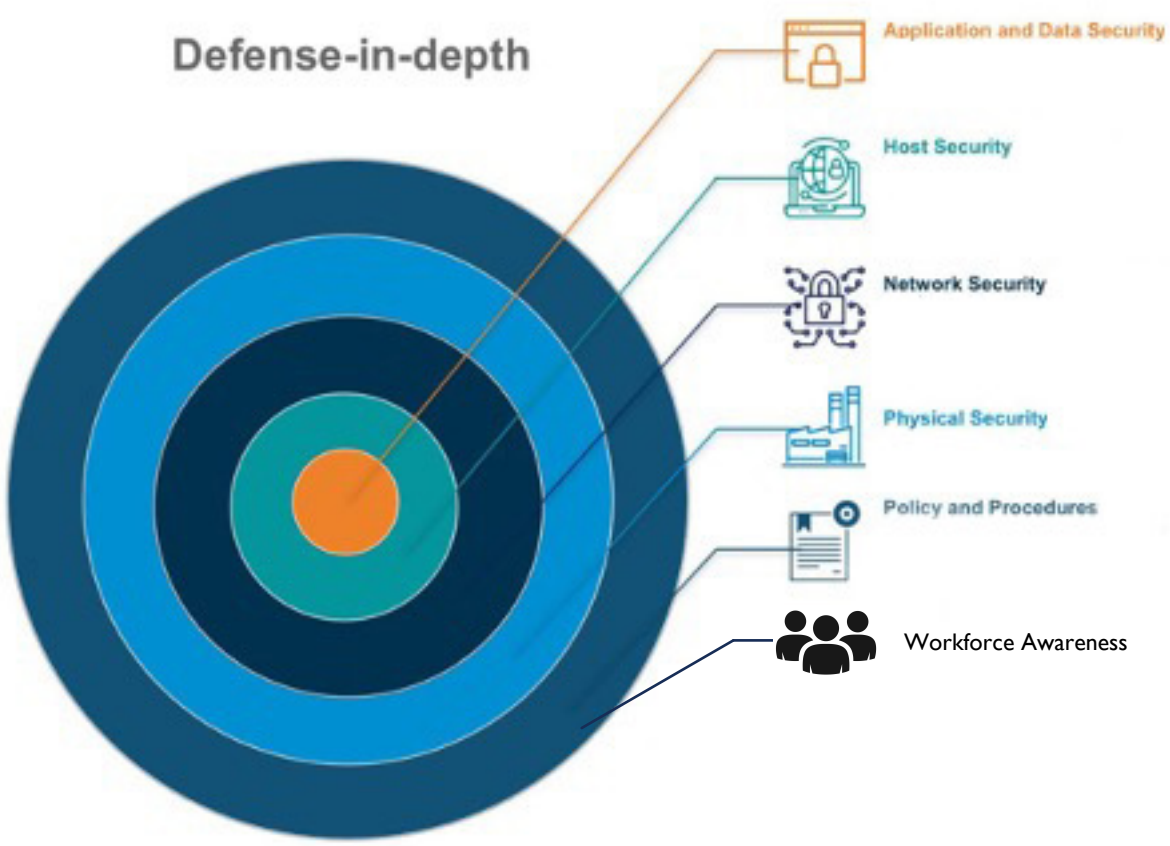


Mission Critical Global Alliance

NRWA

WATER ISAC

DEFENSE-IN-DEPTH



WORKING WITH VENDORS

- Disgruntled employees with malicious intent
  - Maroochydore (2000) – disgruntled former contractor stole equipment and manipulated pumps remotely to discharge sewage into the environment
  - Pennsylvania (2013-14) – disgruntled former employee reprogrammed base stations used in AMR systems for multiple water systems
- Inadequate training or awareness
  - Unintentional error (e.g. configuration error)
  - Lack of awareness (e.g. use of removable media without anti-virus check)
- Lack of adequate processes or procedures
  - Unable to restore to working conditions due to lack of backup
  - Poor account management at vendor exposes organization
  - No incident response plans in place

THREE KEY ACTIONS

- Train **everyone** in your organization regularly to look out for social engineering attacks
- **Test** everyone regularly

Train

- Understand **your** risk
- Reduce **your** risk

Secure

- Create a **real** incident response plan
- Test **your** plan regularly

Prepare

Mission Critical Global Alliance

NRWA

WATER ISAC

QUESTION

- What is the MOST LIKELY source of a cybersecurity incident in your water system?

1. Terrorist targeting your systems.
2. Organized crime group targeting your systems.
3. Intentional action by employee or contractor.
4. Accidental action by employee or contractor.

INSIDER THREATS

JENNIFER LYN WALKER, DIRECTOR OF INFRASTRUCTURE CYBER DEFENSE AT WATERISAC

INSIDER THREAT

According to the CERT Insider Threat Center

An insider threat is the potential for an individual who has or had authorized access to an organization's assets to use that access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Mission Critical Global Alliance

NRWA

WATER ISAC

INSIDER THREATS

Types

- Intentional/malicious/coerced
- Unintentional/accidental/negligent
- Workplace violence

Goals/Outcomes (malicious)

- Intellectual property theft
- Espionage
- Sabotage
- Fraud

INSIDER THREATS & CULTURE

People problem

Organizational-level threat

Address from recruitment through separation

INSIDER THREAT – RECENT EXAMPLES

SECURITY & RESILIENCE UPDATE

Stay current. Stay informed. Stay alert.

THE UNITED STATES ATTORNEY'S OFFICE
DISTRICT of KANSAS

HOME | ABOUT | NEWS | MEET THE U.S. ATTORNEY | DIVISIONS | PROGRAMS

U.S. Attorneys » District of Kansas » News

Department of Justice

U.S. Attorney's Office

District of Kansas

SHARE

FOR IMMEDIATE RELEASE — Thursday, October 21, 2021

Kansas Man Pleads Guilty to Water Facility Tampering

TOPEKA, KAN. – A Kansas man pleaded guilty to tampering with the computer system at a drinking water treatment facility in Ellsworth County. Wyatt Travnichek, 23, of Lorraine pleaded guilty to one count of tampering with a public water system and one count of reckless damage to a protected computer system during unauthorized access.

According to court documents, the Post Rock Rural Water District hired Travnichek in January 2018, and his duties included monitoring the plant after hours using a remote login system. Travnichek resigned his position in January 2019. On March 27, 2019, the remote log in system was used to shut down the plant and turn off one of its filters. Investigators established Travnichek's cell phone was used to perpetrate the intrusion, and that the phone was in his possession at the time of the shutdown. He told investigators he was intoxicated and didn't remember anything about the night of March 27, 2019.

(Updated October 21, 2021) Insider Threat – Former Employee Indicted for Unauthorized Computer Access with Intent to Harm a Kansas Public Water District

Author: Jennifer Walker
Created: Thursday, October 21, 2021 - 14:30
Categories: Cybersecurity, OT-ICS Security

Update - October 21, 2021

More details have been revealed about the former employee of the Post Rock Rural Water District (a.k.a., Ellsworth County Rural Water District No. 1) in Kansas who was indicted for unauthorized computer access with intent to harm, including an updated plea to guilty.

According to the defendant's account, he doesn't recall anything about the night of March 27, 2019, when he gained unauthorized access to the plant's systems, due to his intoxication at the time. But what is more important, it has been confirmed that his unauthorized access was due to his use of shared credentials. Specifically, a shared

Human Error Led to Massive Valdosta Sewage Spill

Share with friends

VALDOSTA, Ga. – On Tuesday, December 10, Darryl Muse, director of City of Valdosta Utilities Department, met with members of the press to discuss the latest raw sewage spill which occurred in the last week.

"It happened at one of the major stations constructed there five years ago to handle the flow," Muse said of the station located behind the newest apartment complex in Remerton off of Baytree.

The City of Valdosta worked with the Department of Health in Florida to issue a joint health advisory to Hamilton and Madison Counties Monday about the 7.5 million gallons of raw sewage that had been released.

Mission Critical Global Alliance

NRWA

WATER ISAC

TIPS TO TACKLE INSIDER THREATS

Deter

- Set expectations through positive culture
- Establish and enforce policies/procedures
- Enforce separation of duties and least privilege account access

Detect

- Involve multiple disciplines within the utility
- Recognize behavioral indicators/stressors
- Apply technical solutions such as auditing/logging/monitoring employee accounts

PRACTICAL ACTIONS TO MITIGATING INSIDER THREATS

Perform a thorough background investigation for potential employees.

Train all new employees (and trusted partners) in security awareness, including insider threats, before granting access to buildings or systems. This should include janitorial and maintenance staff for security situations they may encounter, such as social engineering, active shooter, and sensitive documents left out in the open.

Encourage the reporting of and investigate suspicious behavior.

Consider offering an Employee Assistance Program to help staff deal with stress before it results in a negative action against your utility.

QUESTION

- What types of individuals represent an insider threat to your water or wastewater utility? (select all that apply)
  - Cyber criminals
  - Contractors/vendors/consultants/integrators
  - Employees
  - State-sponsored threat actors
  - Former employees

PHYSICAL SECURITY

ANDREW HILDICK-SMITH, ADVISOR AT WATERISAC

PHYSICAL SECURITY OF YOUR COMPUTER SYSTEMS

If an adversary can touch a piece of your IT or OT equipment or network, they can own it.

Physical Security Principals

- Defense-in-depth
- Deter, Detect, Delay, Deny

OT Computer and Network Hub

THINGS TO PHYSICALLY PROTECT

- PCs and Servers
- **USB and network ports**
- Power and reset switches
- Network cables and equipment
- 3rd Party communication demarcs
- Detailed network and SCADA system documentation on paper
- Password sticky notes under the keyboard?

USB and network ports

PROTECT THE PERIMETER WITH

Standard utility physical security approaches include:

- Guards
- Fences and Gates
- Chains and padlocks
- Site lighting
- Card access
- Intrusion and motion alarms
- Video monitoring

Thermal video image

PROTECT EQUIPMENT WITH

IT and OT equipment can be protected with:

- Locked server rooms with video monitoring
- Locked SCADA cabinets with intrusion alarms
- Locked computer enclosures
- Conduit for network cables
- Disable AutoPlay and AutoRun
- Software Restriction Policy (block ≠ C:\)
- Limiting powershell, cmd and run commands to admin accounts

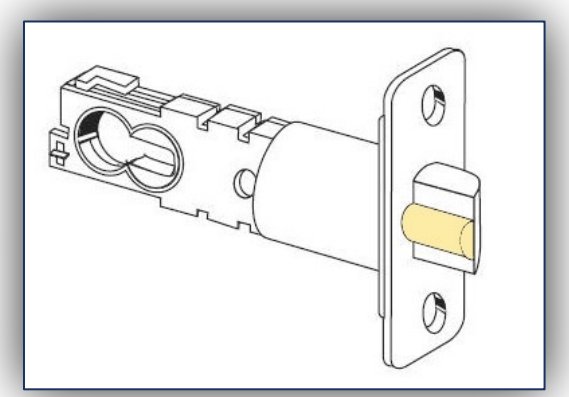
Cage protecting telecomm demarc

PHYSICAL SECURITY WEAKNESSES AND THREATS

Check your physical security. Weaknesses can include:

- Weak locks (pick, drill & cut)
- Lock bypass
- Accessible Request-To-Exit
- Door hinge on the outside

Battery powered grinder



Dead-latch, Schlage

Difluoroethane gas

Mission Critical Global Alliance

NRWA

WATER ISAC

PHYSICAL SECURITY WEAKNESSES AND THREATS, cont.

Weaknesses can also include:

- Lever-style door handle
- Access-card cloning
  (low frequency proximity card)
- Furtive network access
- Exposed network at remote sites

LF prox card duplicator

Drone

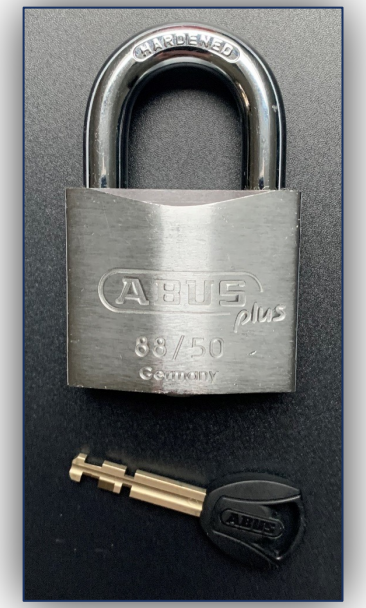
Keyboard emulation tool

PHYSICAL SECURITY IMPROVEMENTS

Possible Improvements:

- Pick resistant locks
- Hardened chains
- Tougher padlocks & shrouds
- Door hinge jam pins
- Astragals and dead-latch engaging
- Clone-resistant access cards
- Staff training on "Tailgating" & reporting

Access card w/ multiple technologies



Pick resistant padlock

Mission Critical Global Alliance

NRWA

WATER ISAC

PHYSICAL SECURITY RECOMMENDATIONS

Help protect computer assets from unauthorized physical access by:

- Keeping doors and panels locked
  - This may require improved ventilation for people and equipment
- Limiting authorized access
- Training staff and building up a physical security culture with:
  - "If You See Something, Say Something"® campaign
  - "Tailgating" training
- Considering a physical penetration test

QUESTION

- Does physical security play an important role in cybersecurity?
  - Yes
  - A little bit
  - Not really
  - No
  - Not sure

RESOURCES

CYBERSECURITY RESOURCES – INSIDER THREAT

- CERT National Insider Threat Center, Common Sense Guide to Mitigating Insider Threats, Sixth Edition https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644
- CISA Insider Risk Mitigation Self-Assessment Tool https://www.cisa.gov/news/2021/09/28/cisa-releases-new-tool-help-organizations-guard-against-insider-threats
- National Insider Threat Task Force (NITTF) https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- National Insider Threat Awareness Month (NITAM) – annually in September
- Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective https://www.dni.gov/files/NCSC/documents/nittf/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021updated-5Apr21b.pdf

CYBERSECURITY RESOURCES – PHYSICAL SECURITY

- DHS, If You See Something, Say Something Campaign®, https://www.dhs.gov/see-something-say-something
- Deviant Ollam, "The Search for the Perfect Door", https://www.youtube.com/watch?v=4YYvBLAF4T8
  (excellent physical security video that includes water utility examples, 1.2 million views)

CYBERSECURITY RESOURCES - GENERAL

- WaterISAC membership, https://www.waterisac.org, ($100/year if <= 3,300 people served. The fee increases with utility size and whether there is both water and wastewater service)
- DHS CISA Cyber Hygiene services, https://www.cisa.gov/cyber-hygiene-services
  - Vulnerability Scanning
  - Phishing Campaign Assessment
- EPA's Free Cybersecurity Assessment and Technical Assistance, etc.
  https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector
  You can register for the free service at, http://www.horsleywitten.com/cybersecurityutilities

CYBERSECURITY RESOURCES - GENERAL, cont.

- NRWA Cybersecurity web page, https://nrwa.org/issues/cybersecurity/
- MS-ISAC membership (state, local, tribal, territorial), https://www.cisecurity.org/ms-isac/
- DHS CISA Stop Ransomware Site, https://www.cisa.gov/stopransomware
- Joint Cybersecurity Advisory "Ongoing Cyber Threats to U.S. Water and Wastewater Systems" (CISA, FBI, EPA, NSA), https://www.cisa.gov/uscert/ncas/alerts/aa21-287a

SAVE THE DATE
FUTURE NRWA-WATERISAC WEBINARS

- March 17 – Account Protection
  - Passwords and Account Management
  - Multi-Factor Authentication
  - Remote Access
- April 14 – Risk Management
  - Patching
  - Backups
  - Incident Management

Mission Critical Global Alliance

NRWA

WATER ISAC

QUESTIONS

STEVE MUSTARD

smustard@mcgalliance.org

JENNIFER WALKER

walker@waterisac.org

ANDREW HILDICK-SMITH

hildick-smith@waterisac.org

THANK YOU