CHALLENGES, SOLUTIONS, AND LESSONS LEARNED FROM THE U.S. WATER SECTOR

NOVEMBER 7, 2022

2022 National Water and Wastewater Conference

DISCLOSURE

TLP:GREEN = Limited disclosure, recipients can spread this within their community.

Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community.

DISCUSSION

- About WaterISAC
- Challenges, Solutions, and Lessons Learned
  - Cybersecurity
  - Physical Security
  - Natural Disasters
- Governance – U.S. Water Sector Regulatory Frameworks
- Q&A

ABOUT WATERISAC

- Established in 2002 at the urging of the White House, FBI, and EPA
- Dues-based, non-profit
- 500+ Members: Utilities, consulting firms, government agencies
- Members in the U.S., Canada, and Australia
- Board members: Utility managers and a state primacy agency administrator

ABOUT WATERISAC

Mission: Protect water and wastewater utilities by providing information and tools for preventing, responding to, and recovering from all hazards.

- Cybersecurity
- Physical Security
- Natural Disasters

INFORMATION GATHERING, CURATION, ANALYSIS & DISSEMINATION

20 YEARS | WATER ISAC

CHALLENGES, SOLUTIONS, AND LESSONS LEARNED

- Cybersecurity
  - Remote Access Incidents
  - Ransomware Incidents
- Physical Security
  - Domestic Violent Extremism
  - Workplace Violence / Insider Threat
- Natural Disasters
  - Historic Rain and Flood Events
  - Extreme Heat, Drought, and Wildfires

CHALLENGES, SOLUTIONS, AND LESSONS LEARNED – CYBERSECURITY

- Remote access incidents
  - Kansas, March 2019
  - California, January 202
  - Florida, February 2021
- Mitigations
  - Use strong passwords
  - Require multi-factor authentication (MFA)
  - Manage access (e.g., allow only for users with a verified need)

"Where there's a wire, there's a way!"

University of South Florida

Department of Justice

U.S. Attorney's Office

District of Kansas

SHARE

FOR IMMEDIATE RELEASE

Wednesday, March 31, 2021

INDICTMENT: KANSAS MAN INDICTED FOR TAMPERING WITH A PUBLIC WATER SYSTEM

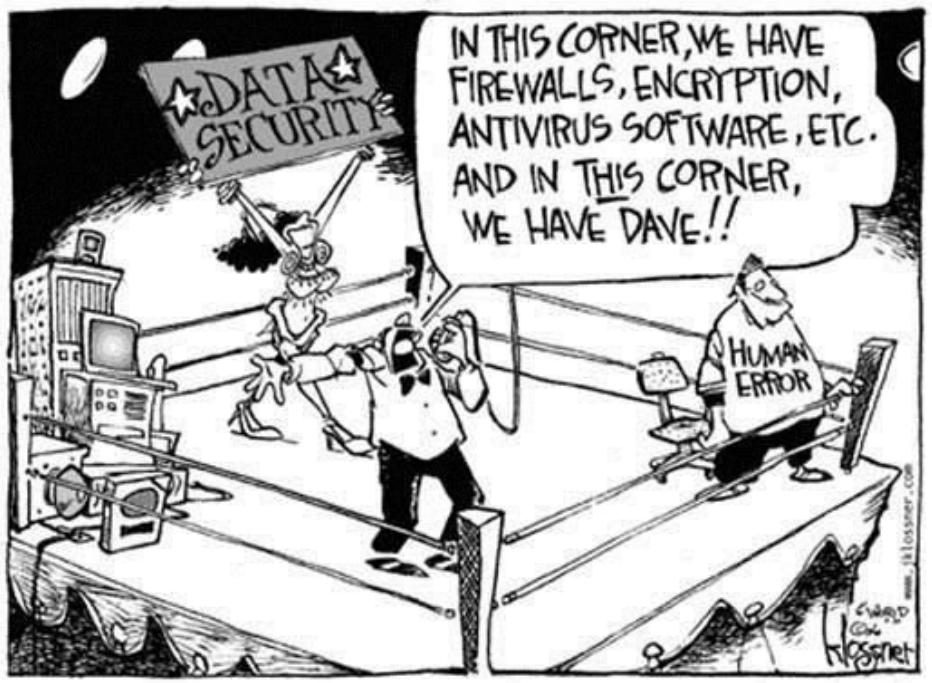
TOPEKA, KAN. – A Kansas man has been indicted on a federal charge accusing him of tampering with a public water system, Acting U.S. Attorney Duston Slinkard said today.

U.S. Department of Justice

20 YEARS | WATER ISAC

CHALLENGES, SOLUTIONS, AND LESSONS LEARNED – CYBERSECURITY

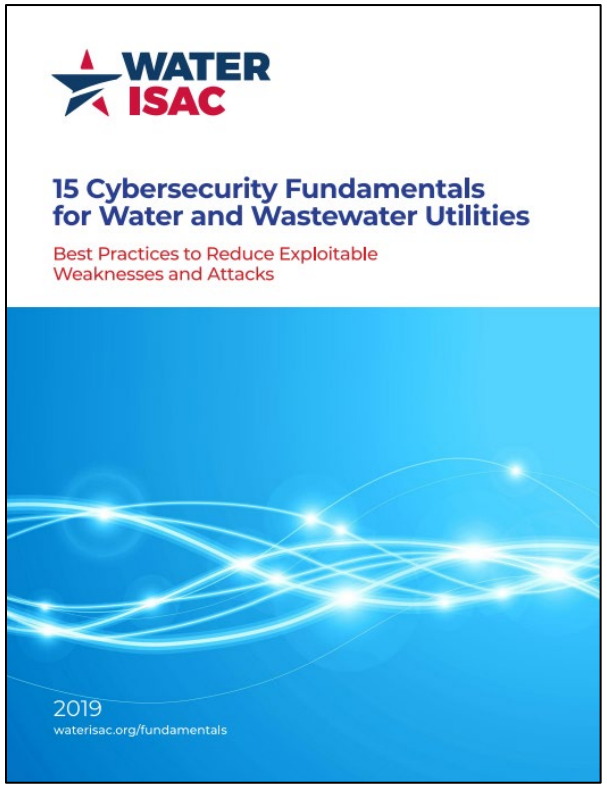
- Ransomware incidents
  - Massachusetts, October 2020
  - Maine, April and July 2021
  - United Kingdom, August 2022
- Mitigations
  - Train employees to spot phishing
  - Conduct regular vulnerability scans
  - Regularly patch and update systems
  - Maintain offline, encrypted backups
  - Have an incident response plan



20 YEARS | WATER ISAC

CYBERSECURITY RESOURCES

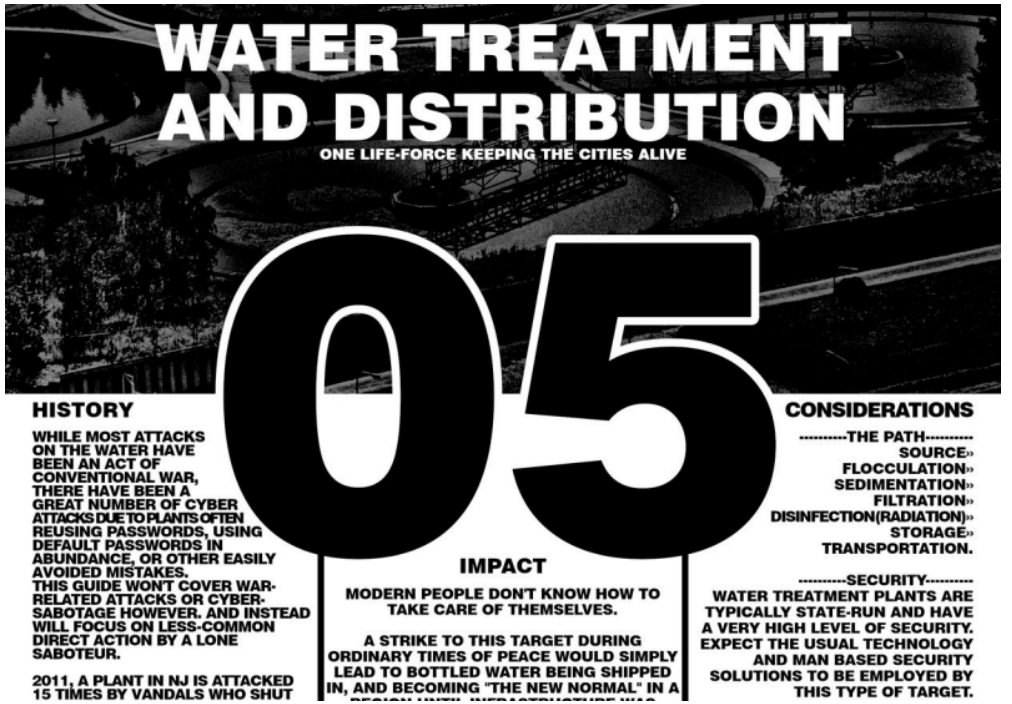
- *15 Cybersecurity Fundamentals for Water and Wastewater Utilities* (WaterISAC)
- Water and Wastewater Cybersecurity Incident Case Studies (WaterISAC)
- *Ongoing Threats to U.S. Water and Wastewater Systems* (CISA, FBI, EPA)
- Known Exploited Vulnerabilities Catalog (CISA)
- MITRE ATT&CK for ICS (MITRE)
- *The ICS Cybersecurity Field Manual – Vol. 1* (SANS)



20 YEARS | WATER ISAC

CHALLENGES, SOLUTIONS, AND LESSONS LEARNED – PHYSICAL SECURITY

- Domestic Violent Extremism
  - Georgia, February 2014
  - Maryland, November 2021
  - Online publications, June 2021 to July 2022
- Mitigations
  - Train personnel to look for indicators of a possible hostile event
  - Maintain vigilance, and report suspicious activities to law enforcement
  - Join information sharing communities



The Hard Reset: A Terrorgram Production

20 YEARS | WATER ISAC

CHALLENGES, SOLUTIONS, AND LESSONS LEARNED – PHYSICAL SECURITY

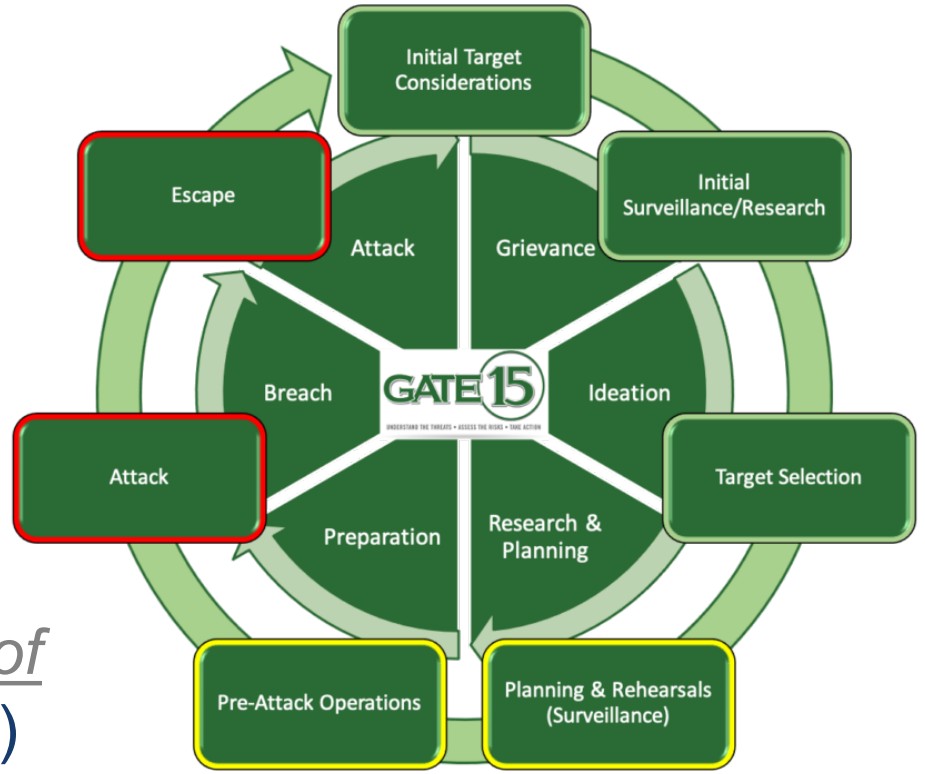
- Workplace Violence / Insider Threat
  - Virginia, May 2019
- Mitigations
  - Establish an insider threat mitigation program
  - Develop an incident response plan
  - Train employees on threat indicators
  - Conduct exercises

*"On average, each active shooter displayed **4 to 5** concerning behaviors over time that were observable to others around the shooter. The most concerning behaviors were related to the active shooter's **mental health, problematic interpersonal interactions, and leakage of violent intent**."*

FBI: *A Study of Pre-Attack Behaviors of Active Shooters in the United States Between 2000 and 2013*

PHYSICAL SECURITY RESOURCES

- The Hostile Event Attack Cycle (Gate 15)
- Recognize Suspicious Activity (U.S. DHS)
- Insider Threat Mitigation Resources (CISA)
- Active Shooter Preparedness (CISA)
- Active Shooter Safety Resources (FBI)
- *An Independent Review of the Tragic Events of May 31, 2019* (The City of Virginia Beach, VA)



Gate 15: The Hostile Event Attack Cycle (HEAC), 2021 Update

CHALLENGES, SOLUTIONS, AND LESSONS LEARNED – NATURAL DISASTERS

- Historic Rain and Flood Events
  - Montana, June 2022
  - Mississippi, August 2022
  - Florida, September 2022
- Mitigations
  - Engage in proactive planning
  - Incorporate environmental justice into decision making
  - Participate in mutual aid networks

City of Billings via AP

20 YEARS | WATER ISAC

CHALLENGES, SOLUTIONS, AND LESSONS LEARNED – NATURAL DISASTERS

- Extreme Heat, Drought, and Wildfires
  - Widespread, June and July 2022
  - West/Western Plains, Ongoing
  - Colorado, January and March 2022
- Mitigations
  - Understand implications of extreme heat on staff and infrastructure
  - Review case studies and best practices
  - Develop contingency plans for loss of access and operations

The Los Angeles Times

20 YEARS | WATER ISAC

NATURAL DISASTER RESOURCES

- Black Sky Resources (WaterISAC)
- *How Two California Water Utilities Responded to a Public Safety Power Shutoff* (WaterISAC)
- Adaptation Case Studies for Water Utilities (U.S. EPA)
- *It's Hot and Getting Hotter: Implications of Extreme Heat on Water Utility Staff and Infrastructure and Ideas for Adapting* (AMWA and WUCA)
- *Drought Management Planning: A Guide for Water Providers* (Wood Environment & Infrastructure Solutions and INTERA)
- *Wildland Urban Interface: A Look at Issues and Resolutions* (FEMA)

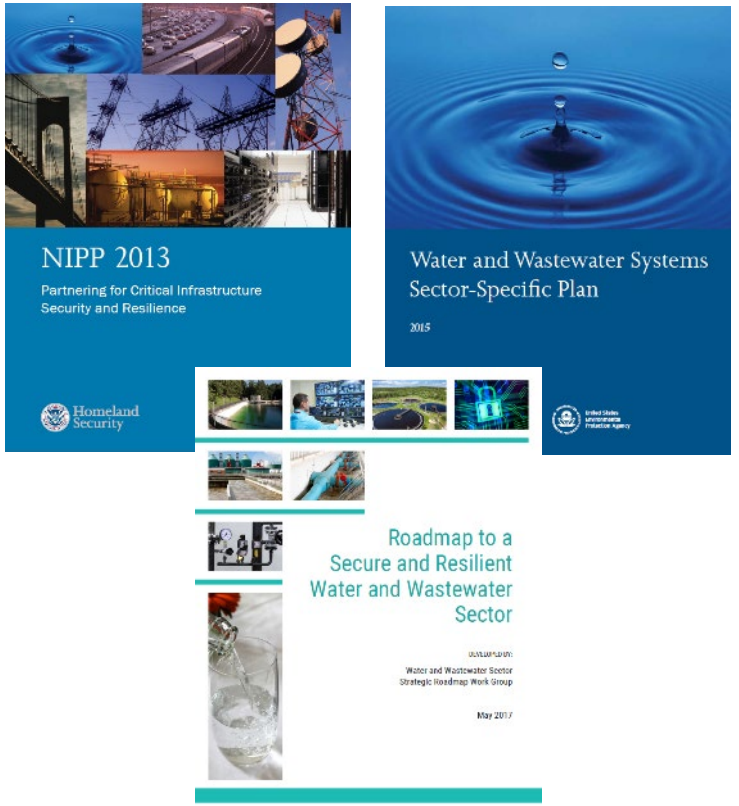
PARTING THOUGHTS

- COMMUNICATE!
- Cultivate a culture of security
- Find a security CHAMPION!
- Train and exercise, and complete after-action reports
- Take advantage of free resources
- Don’t forget about security for small systems

20 YEARS | WATER ISAC

GOVERNANCE – U.S. WATER SECTOR REGULATORY FRAMEWORKS

- Federal environmental laws
  - Safe Drinking Water Act, Clean Water Act, Clean Air Act
  - Enforced by US EPA and state primacy agencies
- Bioterrorism Preparedness and Response Act of 2002
- America's Water Infrastructure Act (AWIA) of 2018
- "Partnership model" for security
  - U.S. DHS and U.S. EPA
  - Water Sector Coordinating Council



20 YEARS | WATER ISAC

H2OSECCON

H2OSecCon VIRTUAL 2022

- Nov 15 – 17, 12:30 to 5 pm ET
  - Covers physical security, cybersecurity, and natural disaster preparedness
  - Two exercises
- Registration:
  - https://www.h2oseccon.org/
  - Water and wastewater utilities that serve < 20,000 individuals, email events@waterisac.org for a complimentary registration.

20 YEARS | WATER ISAC

CONTACT INFORMATION

60-DAY FREE MEMBERSHIPS AVAILABLE!

Website | www.waterisac.org
Incident Reporting Form | https://www.waterisac.org/report-incident
24 Hour Line | 866-H2O-ISAC
Email | analyst@waterisac.org

Chuck Egli
Director of Preparedness and Response
egli@waterisac.org

Jennifer Walker
Director of Infrastructure Cyber Defense
walker@waterisac.org

Alec Davison
All Hazards Threat Analyst
davison@waterisac.org

20 YEARS | WATER ISAC