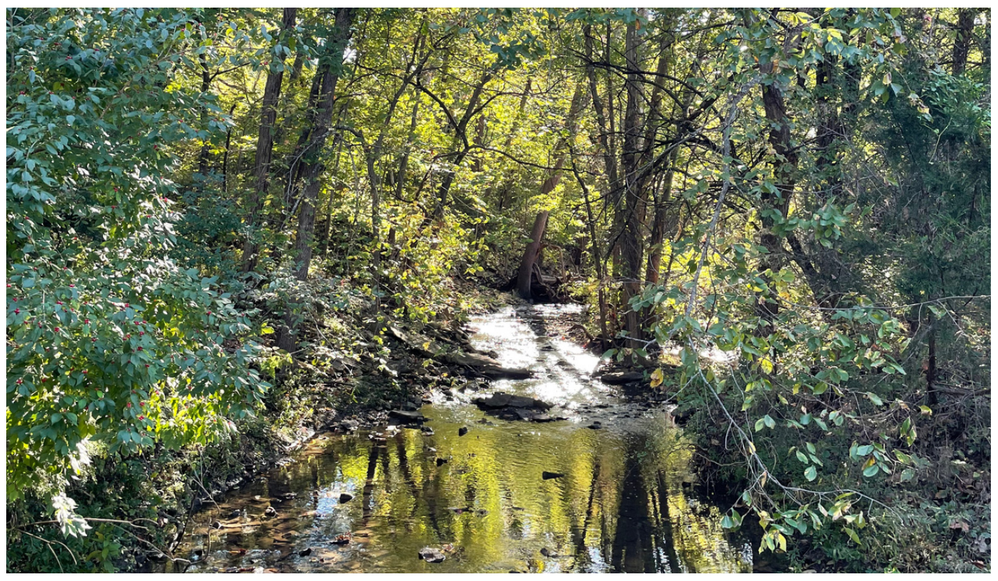
CYBERSECURITY THREATS TO KANSAS WATER SYSTEMS

Alexandra Finley (alexandrafinley@ku.edu)

INTRODUCTION

Kansas is highly susceptible to water system cyberattacks. Water systems, while critical, remain extremely vulnerable. A vulnerable water system leaves the population and economy in a precarious position. Therefore, Kansas has a responsibility to address and mitigate vulnerabilities that affect its water quality and quantity.



THE VALUE OF WATER SYSTEMS

The state of Kansas supports approximately 1,000 water systems. Kansas water systems range from multi-family set-ups to metropolitan utilities. The systems support approximately 2.9 million Kansans and their endeavors.

A large portion supports agriculture. In 2017, 2.8 million acre feet of water was applied to 3.1 million irrigated acres. Water is extremely important to agriculture and agriculture is extremely important to the Kansas economy. Kansas agriculture accounts for 45% of the Kansas economy and supports around 12–15% of the total Kansas workforce. Kansas ranks in the top ten among other states for both agricultural production and exporting. As a result, Kansas water systems also impact foreign markets and investment.

WATER SYSTEM ISSUES

Areas of rural Kansas share water system operators. A water system operator covering more than one municipality increases the risk of multiple communities being affected by cyber infiltration. This amplifies risk since contaminated water sources already risk contaminating other bodies of water due to the natural migration of water.

Additionally, current qualifications for a water system operator generally only require a high school diploma (or equivalent) and a driver's license. However, applications for water system operators in Kansas list a plethora of technical responsibilities. A water system operator must be capable of discovering system comprises, addressing associated risks, and recovering and communicating those risks.

A rural county mitigation action plan require the county to address potential concerns like terrorism. However, many rural municipalities list terrorism as a low concern and do not have current mitigation plans due to a lack of staffing, funding, or both. Mitigation plans tend to prioritize and focus on threats such as natural disaster, impaired water sources, and aging water and wastewater systems. Furthermore, metropolitan water systems remain at the forefront of concern, leaving rural communities without much guidance. A lack of reporting further contributes to this.

RECOMMENDATIONS

- In order to stay up-to-date with technology changes, water system operators should attend yearly, mandatory training regarding water system vulnerability.
- The training should be available online, discuss resources, and include mock cyberattack scenarios to simulate proper procedures and responses.
- The trainings should differentiate between rural and metropolitan communities in order to address different concerns and include a forum for discussion and reporting of cyberattacks and how to address them at each level.
- The training should provide information regarding well-established support programs, pilot programs, specialists, and loans available through the state and federal government.
- Implement a mandatory background check for water system operators and guidelines for revoking access.
- Communities look into potential redundant and back-up systems that mitigate against drought and are not as vulnerable to cyberattacks.
- Increase public awareness and individual preparedness.