DRIVING THE BLUE ECONOMY
TEXAS A&M UNIVERSITY AT GALVESTON

BREAKBULK EDUCATION DAY

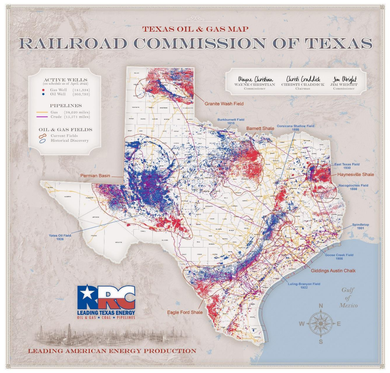
HOUSTON MARITIME Center & Museum

Abstract

Texas remains one of the critical energy hubs in the world. Any disruption to the energy supply will have serious consequences. This may include an increase in energy cost, national security vulnerability, and the cost of groceries. In this poster, a model is developed to predict the level of risk faced by an energy servicing company in the Houston area. The type of cyber-attack chosen was ransomware, which is the most dominant type of cyber-attack in this area. The model relies on Bayesian statistics, which is developed into a graphical model. The Bayesian Network was chosen because maritime cyber-attacks keep getting sophisticated, and so there is a need for a tool that is dynamic and can be updated when new information becomes available. The model uses data from MCAD (Maritime Cyber Attack Database) and is applied to the famous Halliburton ransomware attack of 2024. The results show that across all scenarios, the most consistent risk factors are unpatched systems and gaps in employee training. This means that companies need to keep their systems updated and invest in the training of their employees. In addition, there is also an urgent need to design a comprehensive cybersecurity framework that would counter some of these threats. This study is essential for emergency response, allocating resources, and planning for maritime-related companies.

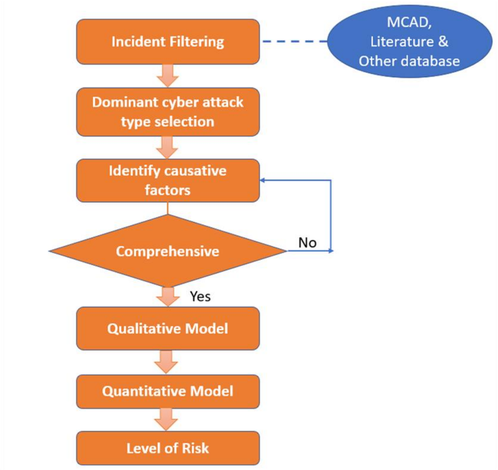
Problem Statement

- Cyberattacks in the maritime industry are increasing rapidly.
- Nearly 92% of the total economic costs from cyberattacks remain uninsured, leaving a substantial financial gap.
- Many companies avoid reporting incidents due to reputation and regulatory concerns.
- Human factors (phishing, weak training, poor cyber hygiene) remain the top vulnerability.
- Cargo handling, vessel navigation, and port operations can be halted, causing global supply chain delays.



https://www.rrc.texas.gov/media/a1yloqcb/ogm0156.jpg

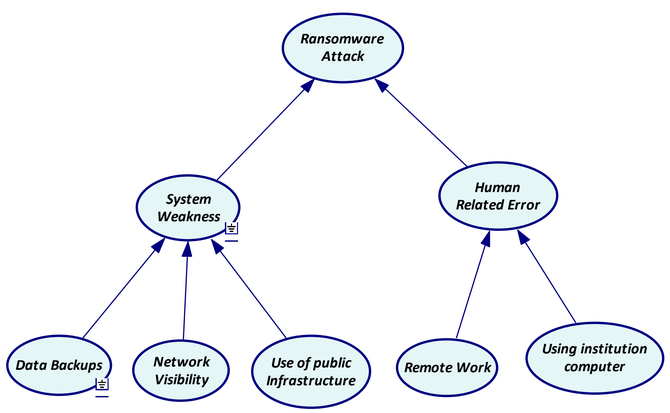
Methodology



$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}$$

Risk= f (Probability, Consequence, scenario, strength of probability)

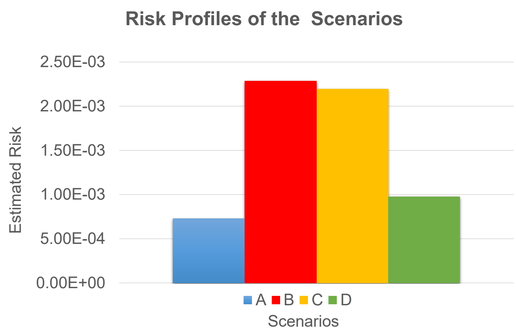
Model



Case-Halliburton Ransomware Attack

Results

SL	Scenario	Estimated Risk
A	System updated, Data has backup, Network visible, Use public infrastructure	7.28E-04
B	System not updated, Data has no backup, no Network visible, Use public infrastructure	2.29E-03
C	Work remotely, Employee not trained, Use institution computer	2.19E-03
D	Using institution computer, Employee trained, Work remotely	9.77E-04



- Scenario B presents the highest ransomware risk due to outdated systems, lack of data backups, limited network visibility, and potential reliance on public infrastructure
- Scenario C highlights human factors—such as insufficient employee training and remote work practices—as the primary risk drivers. Emphasizing staff training and secure remote protocols can substantially lower overall risk.
- Scenario D shows a workforce that is well-trained but primarily working remotely.

Across all scenarios, the most consistent risk factors are unpatched systems and gaps in employee training.

Conclusion

- Ransomware poses a critical threat to maritime resilience.
- For high-value hubs like Houston, robust cyber defense strategies, employee training, and international policy coordination are essential to protect global trade.
- Strengthening preparedness today reduces the risk of devastating economic and safety consequences tomorrow.

Key References

Afenyo, M., Caesar, L.D. (2023). Maritime cybersecurity threats: Gaps and directions for future research, *Ocean & Coastal Management* 236:106493 https://www.sciencedirect.com/science/article/pii/S0964569123000182

Mraković, I. and Vojinović, R. (2019) "Maritime Cyber Security Analysis – How to Reduce Threats?", Transactions on Maritime Science. Split, Croatia, 8(1), pp. 132–139. doi: 10.7225/toms.v08.n01.013. https://www.toms.com.hr/index.php/toms/article/view/250?articlesBySimilarityPage=2#articlesBySimilarity

Project Title: Maritime Cyber risk model for an energy servicing company

Student Name: Swarna Biswas
Faculty Advisor: Dr. Mawuli Afenyo
University Name: Texas A&M University- Galveston
Industry Advisor: John Hark, Director- North America Bertling Logistics

TEXAS A&M UNIVERSITY GALVESTON CAMPUS