Top of Form

|  |  |  |
| --- | --- | --- |
| **Client:** | Dr. Joseph Beckman | **File:** 24-031 |
| **Dept:** | Cybersecurity Technical Assistance Program (TAP/cyberTAP) | **Faculty:**  **Student:** |
| **Date:** | 3/27/2024 | **Initial Meeting:**  **Follow-up:** |
| **Consultant and Attendees:** Sumeeth Guda, Dr. Joseph Beckman, Dr. Chong Gu | | |
| **Statement of Problem:** To determine how best to put local governments in contact with top tier cybersecurity experts in order to strengthen Indiana’s cybersecurity. | | |
| **Goal of this Project:** Journal Article, Grant Proposal, and Technical Report. | | |
| **Background:** The client is a researcher with CyberTap interested in analyzing cybersecurity safeguard implementations among IoT technologies. Their research is funded with a grant under the Indiana Local Government Assessment Program from the Indiana Office of Technology.  They aim to provide data-driven analysis to the Indiana Office of Technology (IOT) supporting recommendations for action by IOT to advance cybersecurity postures among Indiana's local governmental entities. They created a survey and sent it to Indiana local governments concerning cybersecurity safeguard implementations. The ratings scale of the implementations is qualitative – {Not Implementing, Developing, Implementing, Optimizing}. They are evaluating several qualitative and quantitative factors attempting to determine what factors, if any, are predictive of strong cybersecurity postures as defined by the previously mentioned ratings scale.  The end goal of their study is to create statistical metrics to support recommendations to the Indiana Office of Technology regarding how it can best interact with Indiana local governments to move cybersecurity posture forward in that environment. Specifically with putting local governments in contact with top tier cybersecurity experts, and provide them with practical, prioritized advice about doable, powerful cybersecurity fundamentals in order to make Indiana more secure in the short term and shape the state collective cybersecurity strategy and policy in the long term. | | |
| **Progress of project at this time:**  Presently collecting data | | |
| **Relevant information presented at the meeting:** In the meeting, the client briefed Sumeeth and Dr. Gu about the project. The purpose of the project was collecting cybersecurity posture data from various government municipality entities in the state of Indiana and giving each of the factors a rating from 0 to 3. A rating of 0 indicates the cybersecurity feature is not implemented and 3 is the cybersecurity feature is implemented and is continuously being updated and optimized. From each of the municipalities, they aggregated the scores and created a stacked bar chart showing how effective each municipality is using cybersecurity technologies. With this information, once the client finished their assessment for the entity, they produced a descriptive quantitative report for the entity solely and included a short list of recommendations for the entity to complete. Once the project is complete, they will take the aggregated data and provide the information to the Indiana Office of Technology maintaining the confidentiality of the entities. This report will contain the statistical analysis for the data but also will contain recommendations for what the state can do to assist the local entities develop and improve their cybersecurity infrastructure.  So far, the client has 23 entities who filled out the survey. The collection method was that the client or one of their colleagues travelled to the entities and assessed their cybersecurity posture. Once they finished their collection, they added the findings to their report which puts great emphasis on basic display aggregation of data & descriptive analysis. Since they have limited entities, they didn't have enough points to do inferential analysis, rather they described who fell in what category (transformative 12 or focused 14) in other words they grouped the entities which were approximately had the same development, separating the edge cases (Entities with solid security, and the ones were lacking). At the end of their analysis, they have all of the inferential summary.  The client demonstrated the methods that they were using, and they are not complicated. However, they mentioned that they did not have the in-depth understanding of statistical analysis to complete a more thorough report. They came to the SCS for 2 reasons. The first is to seek validation that their statistical methods are correct and appropriate for their report. The second was to receive help from the consultant to conduct a more thorough analysis using more advanced analysis techniques, and to see if there were any holes in their original analysis method.  Dr. Gu and Sumeeth had a lot of concerns about the client’s project:   1. The client did not have a clearly defined question for their project. Based on their application and throughout the meeting, the client was not clear about their expectations and what they specifically needed help with during this assignment 2. The client’s data was not up to date and synchronized to only include points from a fixed time frame. Furthermore, statistical analysis could not be completed because there were too few data points in the client’s dataset. Doing analysis of which could lead to false inference. 3. The client needed to complete their report by June 2024, however they did not emphasize any deadline to the entities that they are surveying. So ultimately there is a lack of data points for this reason. | | |
| **Recommendations for Design and/or Analysis:**  The client was not clear about their goals and expectations. Hence Dr. Gu and Sumeeth could not give any help to the client’s project design or analysis during this IM. Because the client’s project was all about aggregation and did not have any inferential techniques, Dr. Gu suggested some techniques the client could use since they have a report deadline in June 2024.   1. The client should implement deadlines for the entities to gather their cybersecurity posture information. Deadlines are important to gather the most up-to-data information as it presents a sense of how the future posture will be. It will allow the client to summarize and deliver feedback to the client for security infrastructure improvement. 2. The current state of data collection is they are collecting all the information from the clients one at a time. Instead of collecting the entities one at a time, the client should collect the information from all of the entities at the same time instead of in different years. If the client doesn’t do this, when the client does analysis, the info could be outdated. The data needs to be synchronized so the client can assess the data at the same timepoint. If the collection gap is too large, the client needs to recollect the data which could burden the municipal government entities. 3. The client doesn't know if their data is representative, they should continue to make summaries of the aggregated data. Since they only have 27 data points collected so far, they need to collect data from more entities. Once they collect more data points, then they should consider doing formal analysis on the results. 4. Another big concern was that the client did not have a clearly defined question in place for the consultant. If they are looking for the correlations within their whole data, they should look into the various subsets of the data. The only two things needed are a greater number of data points and a clearly defined question for investigation. 5. Some entities are intertwined with each other i.e. (City government, publicly funded sources). The client should add labels to the data set to show if the data points are from the same overall municipalities or if they are independent from each other. | | |
| **Who will carry out these actions?**  **Client:**   * Define a specific problem for the consultant to solve by deriving insight from the dataset. * Finish collecting more data points from the government entities. Make sure to synchronize the data to the same time frame. * Implement deadlines within their survey and finish collecting the data by a specified date. * Notify the consultant when they have a clearly defined problem and have finished completing their survey.   **Consultant:**   * Work with the client to solve their defined problem. * Follow up with SCS directors to see if a follow up meeting is needed. | | |
| **Status:** Follow up needed. Once the client gets enough data and defines their problem, the consultant will initiate the meeting once contacted by the client. | | |

Bottom of Form