**TEAM 2 - Journal**

Ping-Hsuan Chiang, Ruchika Jain, Sahibpreet Singh, Sai Sreevani Boyapally, Shakeel Saleem, Trisha Chatterjee

**Process**:

**Step 1: Data Preparation**

In the project, our aim was to increase the awareness of cybercrime and visually show its impact specifically on the Healthcare sector. We extracted data from multiple sources and in varied formats- some were CSV while others some had to be scraped from PDF documents. Most of the data was clean, however, we had to pre-process some, so that it could be used for further analysis. We had to extract multi-attribute column values separated by a separator and extract them into different columns. Once we had clean and pre-processed data, we imported it into Tableau for visualization purposes.

**Step 2: Data Visualizations and Storyline**

The storyline contains 27 Dashboards.

The introductory dashboards dive into the topic of “Cybercrimes in Healthcare” by giving the audience a preconceived notion that the “Pandemic Alert” in our title is related to COVID, whereas it was actually the increase of cyber crimes in the Healthcare sector. The initial introductory dashboards depict the increase in cybercrimes in various sectors such as Healthcare, Entertainment,Education, Finance etc. Our team holistically chose to focus on the growing rate of Cybercrimes in the Healthcare sector because we believe in the motto “Lives Matter”. We then created a dashboard which showed us the increase in cybercrimes through the years 2009-2021, with a peak in the year 2015. This was due to a ransomware attack on two major healthcare insurers Anthem and Premera which resulted in the largest theft of medical records.

Then began the major storyline of cybercrimes in Healthcare with a real incident of a baby dying in a hospital due to a ransomware attack and examples of a few other incidents of breaches which happened in the past. We created a dashboard to show the number of individuals affected due to cybercrimes in the Healthcare sector in the USA and the states of California, Illinois and Virginia were the most affected states with a large prevalence of data breaches in their healthcare systems.

The next dash represented the top 10 healthcare providers affected by cyber crimes and Trinity Health is the worst affected with the largest number of data breaches. We also created a dashboard which displays the major entry points of malicious softwares and Network Server was the most common entry point. We then give an overview of the impacts these breaches have on healthcare institutions both financially as well as operationally. This led to healthcare providers prioritizing cyber insurances.

The conclusion of our story depicts the emerging technologies which will aid against cybercrimes in the healthcare industry and investment in security intelligence platforms and threat hunting are the highest, with a hope that one day healthcare industry will be cyber crime free and lives will be saved instead of being put at risk.

**Challenges**:

The first challenge was that we were unsure which direction we should focus on to continue the project as there were many topics associated with cybercrime/ cybersecurity.

Once we decided that we were going to focus on Healthcare, we struggled to come up with a smooth and continuous storyline that could keep the audience engaged throughout our presentation. Yet another challenge was to get our presentation ready for the progress report on October 14. We were a team of 6 and initially we split the work amongst ourselves and worked on it individually. However, a lack of collaboration during the initial few weeks meant that we were not prepared to show our work and lagged behind most of the other teams.

**Solutions:**

We performed secondary research and found a lot of news related to the incidents that impacted the healthcare industry. We then realized the importance of cybersecurity especially during the pandemic. Therefore, we decided to choose healthcare as our target industry for the project. The struggle with the storyline was combated using post-its (sticky notes). We wrote all the topics for which we had found the data. After having done that, we moved around the order of the post-its several times until we had a nice flowing story. Not being able to present our work on the 14th was a setback for all of us. On a positive note, that setback provided the thrust our team needed to start working. We collaborated more frequently over the following week and came up with solid final storyline and dashboards; in time for our scheduled meeting with Professor on October 22nd. We then made the necessary changes that were pointed out by the Professor in the meeting, and were ready for the final presentation on October 28, 2021.

**Sources:**

* <https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465>
* <https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254>
* <https://nypost.com/2021/09/30/alabama-baby-died-from-hospital-ransomware-attack-lawsuit/>
* <https://www.medsphere.com/blog/2017-set-records-hospital-data-breaches/>
* <https://www.paubox.com/blog/over-half-million-trinity-health-patients-affected-data-breach/>
* <https://www.newsweek.com/cyberattack-throws-southern-california-hospital-system-offline-days-1588355>
* <https://www.healthcareitnews.com/news/cancer-patient-sues-ucsd-health-over-500k-record-info-breach>
* <https://www.fiercehealthcare.com/tech/relentless-cyber-attacks-are-putting-pressure-hospital-finances-fitch-ratings>
* <https://www.aoa.org/news/practice-management/perfect-your-practice/healthcare-cybersecurity?sso=y>
* <https://public.tableau.com/app/profile/anna.h.dzikowska/viz/IronQuest1_2019_CyberCrimeinHealthCare/Dashboard1>
* <https://www.zdnet.com/article/cyber-criminals-targeting-hospitals-are-playing-with-lives-and-must-be-stopped-report-warns/>
* <https://www.zdnet.com/article/ransomware-why-these-attacks-could-get-even-more-dangerous-and-disruptive/>
* <https://www.fiercehealthcare.com/tech/relentless-cyber-attacks-are-putting-pressure-hospital-finances-fitch-ratings>
* <https://www.beckershospitalreview.com/cybersecurity/surgeries-canceled-ambulances-diverted-it-system-down-at-ohio-health-system-after-ransomware-attack.html>
* <https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/>
* <https://www.brookings.edu/blog/techtank/2021/08/09/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/>
* <https://www.cpomagazine.com/cyber-security/healthcare-cyber-attacks-rise-by-55-over-26-million-in-the-u-s-impacted/>
* <https://www.fitchratings.com/research/insurance/cyber-theft-of-customer-data-growing-risk-for-us-health-insurers-29-06-2021>
* <https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/>

Datasets

* <https://www-statista-com.ezproxy.lib.uconn.edu/statistics/1237131/cybersecurity-incidents-in-healthcare-organizations-us/>
* Several others all from Statista

Cyber Security:

* <https://www-statista-com.ezproxy.lib.uconn.edu/statistics/1237198/targets-of-cyber-security-incidents-in-healthcare-in-the-us/>
* <https://www-statista-com.ezproxy.lib.uconn.edu/statistics/1237192/impact-of-cyber-security-incidents-in-healthcare-us/>
* Several others from Statista
* Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*. <https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-020-01161-7>