Tentative Abstract:

- Outline
    - Background/Introduction
        - Incident occurred on July 19, 2024
        - Outages only affected Windows computers with the Falcon sensor security software installed
        - Problem attributed to faulty update to the software that caused systems to crash
        - Experts suspected CrowdStrike's testing of patches was not rigorous enough
            - Bug in CS's patch validation software allowed the patch to get through with the severe bug
    - Research Question
        - Did CrowdStrike release timely and accessible communications that served to alert customers and contain the problem? And how did this responsiveness serve to mitigate/worsen the situation and ensure it doesn't happen again?
        - How did CrowdStrike's communications immediately following the incident serve to alert customers and contain the problem? How did this reflect on public perception of CrowdStrike?
    - Methods
        - Examining official report from CrowdStrike
        - Finding timely news articles reporting on the impact
        - Considering both responses from individuals and corporations
        - Looking at Google Search Trends and noting location (D.C. was top geographical location)
        - Finding comprehensive peer-reviewed articles on the specifics of Falcon's inner workings and how the update was able to crash systems
    - Tentative Findings
        - Accessibility of communications was reasonable given the scale of the incident. However, from the lens of a general audience, it is very technically-worded and certain remediation correspondences are convoluted to access (i.e. GitHub repository and using BIOS)
    - Discussion and Recommendations

        - Things that went well: Respond quickly and with an effective solution. Reach out and respond to clients and support lines via multiple different avenues such as: social media, customer support, news, blogs, televised coverage, etc.
- Abstract
    - On July 19, 2024, a mass computer outage affecting a large section of both private and public sector Windows-based computer systems caused major interruptance of service globally, notably presenting issues in which both timeliness and accessible communications with the public are at stake to ensure both past and future mistakes do not occur. The cause of the outage was a faulty update to CrowdStrike’s Falcon sensor cybersecurity software creating constant crashing on affected systems, rendering them unusable. By examining both official and unofficial reports and correspondence from CrowdStrike, we aim to highlight both potential areas of poor communication and proper resourcefulness in their diligent work ensuring a reassuring response. We consider both this perspective in combination with the perspectives of those affected in this incident, such as businesses, to consider if both the effectiveness and appropriateness of CrowdStrike’s remediation response are suitable for their target audience.

Progress Research Summary (1 single-spaced page):

- Sources
    - Primary
        - https://www.crowdstrike.com/en-us/blog/to-our-customers-and-partners/
        - https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/
    - Secondary
        - https://www.bbc.com/news/articles/cr54m92ermgo
            - CrowdStrike: What was the impact of the global IT outage
        - https://edition.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause
    - Peer-reviewed article
        - https://journals.nauss.edu.sa/index.php/JISCR/article/view/3129/1409
- Highlights
    - Challenges
        - Bias
    - Surprising/Useful Findings
- Questions to consider
    - What have you learned about the audiences and genres that were used when communicating about this crisis?
    - How did the specific context of this crisis create challenges for technical communication? (e.g., pressure, controversy, time demands, inequalities/biases)
    - What areas do you think you've fully researched? What do you still need to look more into?
    - How have you been dividing the research? Is that approach working or do you want to make adjustments?
    - What are you having trouble finding that would be helpful to get suggestions or leads on?

To research the CrowdStrike incident, and the communication surrounding it, our pair decided to first examine official communications released by CrowdStrike itself. This gave us context on the actions CrowdStrike took, and how quickly they took them. We used two blog posts made by CrowdStrike in particular: To Our Customers and Partners and Falcon Content Update Remediation and Guidance Hub. The first blog post serves to alert customers and partners to the problem, and state that CrowdStrike has already deployed a fix. It is also meant to dismiss concerns of the outage being the result of a cyberattack. The second blog post has several purposes. It states what caused the outage, gives a guide of how to fix it for customers, and also provides actions CrowdStrike has taken and will take in response to their mistakes. It provides the how-to guide in both written and video tutorial form. These two sources provide a solid basis for us to understand CrowdStrike's response to the crisis.

Additionally, we examined secondary sources released around the time of the incident. An article by CNN discusses the vast impact of the incident, including an estimated $5 billion in losses to Fortune 500 companies, and industries impacted, such as the airline, healthcare, and banking industries. An article by the BBC released two months after the incident discusses the impacts to airlines, healthcare, and small businesses in the UK.

Due to the severe nature of CrowdStrike's mistake, many news articles focus on the negative impacts it had. While this makes sense considering their audience, it neglects to examine the effectiveness of CrowdStrike's communication. This creates an unintended bias which made our research more difficult when looking at secondary sources.

We have also referred to a peer-reviewed article about the incident. It provides many of the technical details behind CrowdStrike's software that is useful to understand how it works. It also discusses the incident itself, and gives its own perspective on what went wrong in CrowdStrike's software development cycle to cause the incident.

In summary, our pair has explored a diverse set of sources to better understand the technical communication surrounding the CrowdStrike incident. Continuing forward, we hope to investigate primary sources from stakeholders and impacted customers and partners.

Research Notes:

https://www.crowdstrike.com/en-us/blog/to-our-customers-and-partners/