

Communicative Efficacy: The 2024 CrowdStrike Incident and Associated Handling of Remediation

Introduction

A mass computer outage caused by a faulty update to CrowdStrike’s Falcon security software caused major interruptance of computer-reliant service on a global scale in July of 2024. Our aim is to analyze and interpret communication from CrowdStrike in this incident. We highlight both potential flaws with the methods of communication, as well as indicate when proper communication occurs. Likewise, both the perceived effectiveness of CrowdStrike’s response and those affected are considered to provide a holistic view on the aforementioned effectiveness.

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?

Methods

To analyze the communications surrounding the outage, we examined:

- Official reports from CrowdStrike
- News articles reporting on the impact
- Responses from individuals and corporations

Results

The public response from CrowdStrike through their official channels and website was professional and included multi-modal forms of communicating reconciliation steps and procedures, especially within their guidance hub. Within the guidance hub, CrowdStrike not only continually updated as solutions and important information rolled out, but also provided concise information with links to more detailed documents. While the means of fixing the software remained obtuse, via YouTube and other documentation, accessing these resources (i.e. GitHub, BIOS, etc.) was easier to digest.

Discussion

We claim that CrowdStrike’s response was effective in managing an incident of this scale and reached out with an effective solution to many affected parties. Both support lines and public-facing communication existed via varying avenues, such as social media, customer support, news outlets, and directed correspondence from Microsoft and other affiliated groups industry-wide. CrowdStrike’s transparent and collaborative approach to releasing their information provides an insight into how to best handle communication intended to address mass hysteria quickly and effectively.

References

- <https://www.crowdstrike.com/en-us/blog/to-our-customers-and-partners/>
- <https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/>
- <https://www.bbc.com/news/articles/cr54m92ermgo>
- <https://edition.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause>
- <https://journals.nauss.edu.sa/index.php/JISCR/article/view/3129/1409>
- <https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/>

