



## The shaky foundation of global technology: A case study of the 2024 crowdstrike outage

Olugbenro Ogundipe <sup>1</sup>, Dr. Tejiri Aweto <sup>2\*</sup>

<sup>1,2</sup> Doctoral Candidate in Business Administration (DBA) | Edgewood College 1000 Edgewood College Dr, Madison, WI 53711, US

\* Corresponding Author: **Dr Tejiri Aweto**

---

### Article Info

**ISSN (online):** 2582-7138

**Volume:** 05

**Issue:** 05

**September-October 2024**

**Received:** 06-07-2024

**Accepted:** 08-08-2024

**Page No:** 106-108

### Abstract

The 2024 CrowdStrike outage serves as a stark reminder of the fragility of our interconnected technological systems. This paper explores the root causes of the outage, its impact on various sectors, and the lessons learned from this incident. By analyzing the events leading up to the outage, the immediate response, and the long-term implications, we aim to shed light on the vulnerabilities of our global technological infrastructure and propose potential solutions to prevent similar disruptions in the future.

The widespread technological outage caused by a CrowdStrike software update in July 2024 exposed the fragility of the interconnected global tech ecosystem. This paper examines the outage's causes, impacts, and implications, arguing that it serves as a stark warning about the vulnerabilities inherent in our increasing reliance on complex, interconnected systems. The incident highlights the need for a comprehensive reassessment of risk management strategies, contingency planning, and the potential for cascading failures within the digital infrastructure that underpins modern society.

**Keywords:** Technological Systems Fragility, Global Tech Ecosystem, Software Update Failure, Contingency Planning

---

### Introduction

On July 19, 2024, a software update from CrowdStrike, a leading cybersecurity company, triggered a global outage that affected millions of Windows-based systems across multiple industries. This incident highlighted the interconnectedness of our digital world and the potential for a single point of failure to have far-reaching consequences. In this paper, we will examine the outage details, its impact on various sectors, and the lessons learned from this event.

The CrowdStrike outage of July 2024, resulting from a faulty update to their Falcon cybersecurity software, was a significant event that disrupted businesses, government agencies, educational institutions, and critical infrastructure worldwide. The outage affected millions of Windows devices, causing widespread system failures and service interruptions. While the incident was ultimately resolved, it exposed the inherent fragility of the global tech ecosystem, raising concerns about the resilience of our increasingly interconnected digital infrastructure.

### Background

CrowdStrike is a prominent cybersecurity company that provides endpoint security solutions to organizations worldwide. On July 19, 2024, a routine software update, Channel File 291, was released by CrowdStrike. This update contained a logic error that caused Windows-based systems to crash, leading to a widespread outage (CrowdStrike, 2024) <sup>[1]</sup>. The outage affected approximately 8.5 million Windows devices, disrupting critical services across various industries (Microsoft, 2024) <sup>[6]</sup>.

### Causes of the Outage

The outage stemmed from an error in a Rapid Response Content update designed to adapt to evolving threats quickly. This update inadvertently triggered a bugcheck\blue screen error on millions of Windows systems running the CrowdStrike Falcon

sensor. The error was not malicious in nature but rather a logic error within the update. The widespread impact of the error underscored the potential for seemingly minor software flaws to have cascading effects across interconnected systems.

### Impact on Various Sectors

The CrowdStrike outage had a significant impact on several sectors, including healthcare, finance, and transportation. In the healthcare sector, hospitals and clinics experienced disruptions in their electronic health record systems, leading to delays in patient care and potential risks to patient safety (Healthcare IT News, 2024) <sup>[5]</sup>. Financial institutions faced challenges in processing transactions and maintaining the integrity of their systems, which could have resulted in financial losses (Business Insider, 2024) <sup>[1]</sup>. The transportation industry also experienced disruptions, with airlines facing flight cancellations and delays due to the outage's impact on their systems (CNN Business, 2024) <sup>[4]</sup>.

### Impacts of the Outage

The outage's impact was far-reaching, disrupting operations across multiple sectors. Hospitals experienced system failures, airlines faced flight cancellations, and educational institutions had to cancel classes. Businesses of all sizes were affected, with many losing productivity and experiencing financial losses. The incident also highlighted the potential risks to critical infrastructure, as some hospitals and government agencies experienced service interruptions.

### Immediate Response and Recovery

CrowdStrike and Microsoft worked together to address the issue promptly. Microsoft released a recovery tool that used a USB drive to boot and repair affected systems, while CrowdStrike provided guidance to its customers to resolve the issue (CISA, 2024) <sup>[8]</sup>. The recovery process was time-consuming, as each affected system required manual intervention to deploy the fix and roll back the problematic update (Lexology, 2024) <sup>[6]</sup>.

### Lessons Learned

The CrowdStrike outage of 2024 serves as a wake-up call for the global technology community. It highlights the need for increased vigilance in software development and deployment processes, as well as the importance of robust testing and validation procedures. The incident also underscores the need for redundancy and backup systems to minimize the impact of a single point of failure. Furthermore, the outage emphasizes the importance of effective communication and collaboration between technology providers and their customers during crisis situations.

### Implications for Global Tech

The CrowdStrike outage serves as a stark reminder of the vulnerabilities inherent in the global tech ecosystem. Our increasing reliance on complex, interconnected systems creates a situation where seemingly minor errors can have disproportionately large consequences. The incident highlights the need for a comprehensive reassessment of risk management strategies, contingency planning, and the potential for cascading failures within the digital infrastructure that underpins modern society.

### Risk Management and Contingency Planning

The CrowdStrike outage underscores the importance of robust risk management and contingency planning within the tech industry. Organizations need to anticipate the potential for failures, even in seemingly reliable systems, and develop plans to mitigate the impact of such events. This includes having backup systems in place, regularly testing disaster recovery procedures, and ensuring that critical personnel are trained to respond effectively to unexpected disruptions.

### Cascading Failures and Systemic Risk

The interconnected nature of the global tech ecosystem creates a risk of cascading failures, where a single incident can trigger a chain reaction of disruptions across multiple systems. The CrowdStrike outage demonstrated this risk, as the initial software error led to widespread system failures and service interruptions across various sectors. This incident highlights the need for a deeper understanding of systemic risk within the tech ecosystem and the development of strategies to mitigate the potential for cascading failures.

### Conclusion

The CrowdStrike outage of 2024 is a significant event that exposed the fragility of the global tech ecosystem. The incident serves as a warning about the potential for cascading failures within our increasingly interconnected digital infrastructure. It highlights the need for a comprehensive reassessment of risk management strategies, contingency planning, and the potential for systemic risk within the tech industry. By learning from this incident, we can take steps to build a more resilient and robust global tech ecosystem.

The 2024 CrowdStrike outage was a significant event that exposed the vulnerabilities of our global technological infrastructure. The incident had far-reaching consequences across various sectors, highlighting the need for increased attention to software development, testing, and deployment processes. By learning from this event and implementing the necessary changes, we can work towards building a more resilient and secure global technology foundation.

### References

1. Business Insider. Why it's taking time for companies to recover from the CrowdStrike IT outage; c2024. Retrieved from
2. CrowdStrike. Statement on the July 19, 2024, outage; c2024. Retrieved from
3. CISA. Widespread IT Outage Due to CrowdStrike Update; c2024. Retrieved from
4. CNN Business. Timeline: How the CrowdStrike outage unfolded; c2024. Retrieved from
5. Healthcare IT News. Healthcare recovering from CrowdStrike outage; c2024. Retrieved from
6. Lexology. CrowdStrike/Microsoft outage: Priority steps for impacted businesses; c2024. Retrieved from
7. Microsoft. Statement on the July 19, 2024, CrowdStrike outage; c2024. Retrieved from
8. CISA. Widespread IT Outage Due to CrowdStrike Update; c2024. <https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due->

- crowdstrike-update
9. Alonso J. How the CrowdStrike Global Technology Outage Affected Colleges. Inside Higher Ed.; c2024. <https://www.insidehighered.com/news/tech-innovation/administrative-tech/2024/07/22/how-crowdstrike-global-technology-outage>
  10. CrowdStrike. Remediation and Guidance Hub: Falcon Content Update for Windows Hosts; c2024. <https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/>