IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, March 2025
Impact Factor: 7.67

Unraveling the 2024 CrowdStrike Incident: How a Security Patch Led to Global System Failure and Blue Screen of Death

Venkata Baladari
Sr. Software Developer, Newark, Delaware
vrssp.baladari@gmail.com

Abstract: *The 2024 CrowdStrike Cybersecurity incident resulted in a worldwide IT disruption impacting millions of Microsoft Windows systems. In July 2024, a faulty update of CrowdStrike's Falcon Endpoint Detection and Response (EDR) software caused widespread system crashes known as the "Blue Screen of Death" (BSOD). The event caused severe disruptions to major industries such as aviation, financial services, healthcare and emergency response systems resulting in operational shutdown, financial setbacks and global safety concerns.*

This study presents a detailed examination of the CrowdStrike incident, focusing on the technical issues, global effects and legal consequences. The research delves into the weakness of centralized cybersecurity systems, emphasizing the dangers of putting too much trust in single-point security services. The research highlights the significance of strict testing protocols, comprehensive cybersecurity frameworks, and risk assessment strategies enhancing future cybersecurity preparedness. The CrowdStrike incident presents a compelling case study in global cybersecurity risk management, prompting organizations to reassess redundancy measures, failover mechanisms, and more decentralized security architectures in order to protect critical IT systems..

Keywords: CrowdStrike, Cybersecurity, Cyber Risk Management, Incident Response, Regulatory Compliance, Blue Screen of Death (BSOD)

I. INTRODUCTION

As companies undergo digital transformation, effective cybersecurity measures have become critical for safeguarding confidential information, thwarting cyber threats, and maintaining uninterrupted business operations. Protecting sensitive data and preventing cyber threats has become essential for ensuring the continuity of business operations within modern digital infrastructure systems. CrowdStrike was established in 2011, one of the leading providers of cloud-based cybersecurity solutions by offering real-time threat intelligence, endpoint security, and malware detection services. CrowdStrike Falcon, a type of Endpoint Detection and Response (EDR) software, is crucial in thwarting ransomware assaults, identifying malicious software, and safeguarding corporate networks. Falcon EDR, is widely utilized by corporations and government agencies to identify and prevent cyber threats [1],[2].

An unprecedented event occurred on July 19, 2024 when a defective software update within the Falcon EDR caused the "Blue Screen of Death" (BSOD) to appear on millions of Microsoft Windows systems, leading to a blackout which was instantaneous and affected various sectors including but not limited to:

- Aviation: failure of airport systems caused flight delays and cancellations impacting millions of travelers
- Financial services: widespread financial disruptions in banks, ATMs and payment systems
- Healthcare: hospitals experienced problems with patient record system causing significant delays
- Emergency response systems: emergency services networks like 911 call centers, first responders networks were impacted instilling fear on public safety

ISSN 2581-9429 IJARSCT
DOI: 10.48175/IJARSCT-24524

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, March 2025
Impact Factor: 7.67

The CrowdStrike outage demonstrated a significant issue, that if not thoroughly tested and accurately deployed, Cybersecurity solutions can themselves cause disruptions. The 2024 incident has triggered discussions about the dangers of putting too much faith in centralized security companies, highlighting the vulnerability of cybersecurity solutions when a flaw in a software update can cause significant cybersecurity failures [1],[3].

The research paper investigates the 2024 CrowdStrike incident by analyzing the underlying reasons leading to the worldwide system failure, assessing the short term and long term consequences, legal and regulatory implications. The study also examines the key takeaways and best practices of future cyber security resilience focusing on diversification and established risk management strategies.

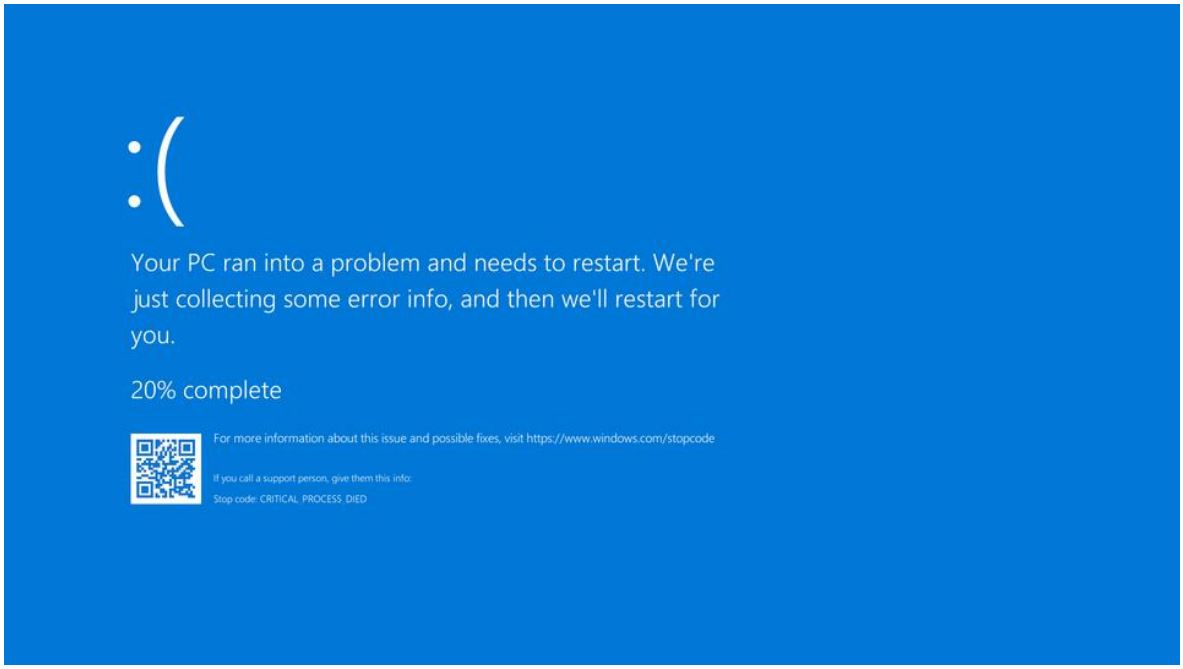

Fig. 1. Blue Screen of Death (BSOD) issue on Windows systems (Accessed from https://en.wikipedia.org/wiki/File:Bsodwindows10.png)

II. CROWDSTRIKE AND ITS ROLE IN CYBERSECURITY

As a prominent Cybersecurity company for the past 10 years, CrowdStrike has focused on providing cloud-based Cybersecurity utilizing artificial intelligence, machine learning and behavioral analytics to identify and neutralize cyber threats. In 2024, CrowdStrike had over 24,000 customers including Fortune 500 companies, government organizations and many more. The company played a key role in threat intelligence, endpoint security solutions, digital forensic services and malware-based threats. CrowdStrike adopts a zero-trust security framework, whereby every endpoint undergoes ongoing verification and surveillance. Some of the key features of CrowdStrike's Cybersecurity Services are:

Falcon Endpoint Detection and Response (EDR): CrowdStrike Falcon EDR engineered to deliver real-time visibility and threat monitoring, detection and response [1].

- **Cloud Security:** CrowdStrike's security solutions enable businesses to scale their cybersecurity operations effectively [1][2].
- **Falcon X threat intelligence:** Falcon X is cloud based platform enabling organizations to protect themselves against real-time ransomware attacks and eliminating the need for on-premises infrastructure [4].

ISSN 2581-9429 IJARSCT
DOI: 10.48175/IJARSCT-24524

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, March 2025
Impact Factor: 7.67

- **CrowdStrike Falcon Adversary Overwatch:** CrowdStrike's OverWatch service offers 24/7 threat hunting service powered by threat intelligence and advanced AI allowing organizations to identify and eliminate complex, long-lasting cyber threats known as Advanced Persistent Threats (APTs) [5].

III. INCIDENT DISCOVERY, KEY DETAILS AND TIMELINES

A. Incident response and key timelines

The 2024 CrowdStrike Incident represented the most severe disruption the company faced. Throughout its history, CrowdStrike has encountered numerous technical challenges, software vulnerabilities, and cybersecurity issues that have substantially impacted its expansion and evolution. On July 19, 2024, millions of Microsoft systems displayed the "Blue Screen of Death" (BSOD) due to a scheduled update implemented by CrowdStrike's Falcon EDR security software. The key sequence of events are shown in Figure 1 [3].

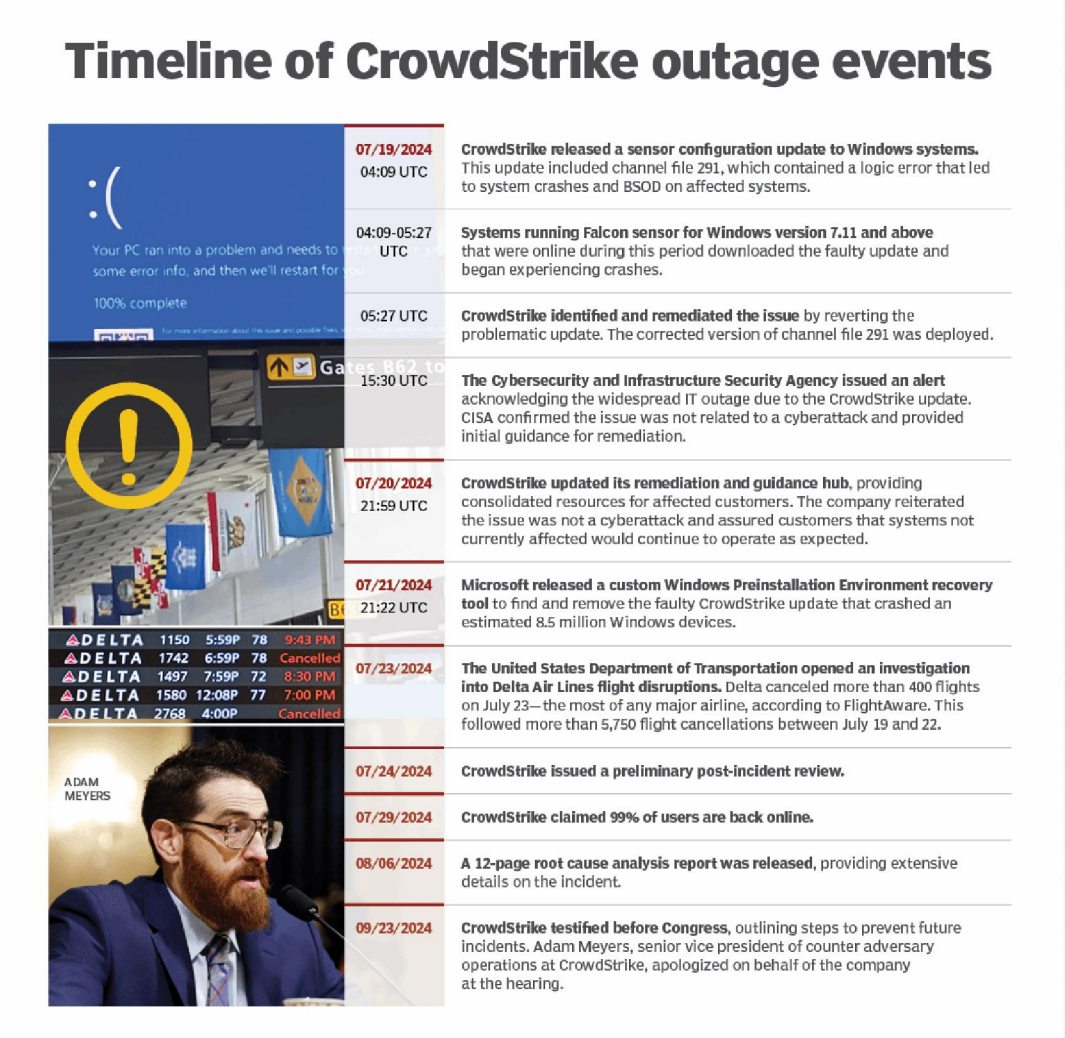

Fig. 2. Critical timelines of CrowdStrike incident (Accessed from : https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next)

ISSN 2581-9429 IJARSCT
DOI: 10.48175/IJARSCT-24524

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 8, March 2025 Impact Factor: 7.67

B. Ramification of the incident on public and private sectors

The incident had a significant impact on various public and private sectors causing substantial financial and operational losses.

- Aviation: failure of airport systems caused flight delays and cancellations impacting millions of travelers. Thousands of flights were cancelled by Delta Air Lines, United Airlines, and American Airlines due to air traffic control and operational system malfunctions. The airline's check-in systems, booking platforms, and baggage handling services were taken offline incurring losses exceeding $1 billion
- Financial services: widespread disruptions in bank transactions, ATMs and payment systems. The trading platforms faced significant disruptions causing stock market volatility.
- Healthcare: hospitals experienced problems with Electronic Health Record (EHR) systems causing access issues to patient medical records. Diagnostic equipment and medical devices were also impacted causing delays in critical care procedures.
- Government agencies and Emergency response systems: emergency services networks like 911 call centers, first responders networks were impacted prompting fear on public safety. Several government offices and local services also experienced IT outages impacting several services.

The extent of the disruption emphasized the fundamental dependance on Cybersecurity solutions and the inherent potential threats with centralized security systems.

C. Post incident actions and Government reforms

The incident severely impacted CrowdStrike's reputation and caused financial repercussions on the company's stock value. CrowdStrike released a formal statement and swiftly implemented mitigation measures to address the issue. Customers were advised to disable Falcon EDR and an emergency patch was released to mitigate the issue. A number of class-action lawsuits were brought against CrowdStrike, alleging lack of diligence in software testing procedures. Regulatory bodies in the US, EU and implemented task forces to guarantee resilience on software validations [6].

IV. CYBER SECURITY STRATEGY AND FUTURE BEST PRACTICES

A CrowdStrike outage prompted cybersecurity executives and companies to reassess their risk management plans. Although the 2024 CrowdStrike incident was unrelated to a cyberattack, it served as a reminder of the potential outcomes of flawed update processes and insufficient testing procedures. Organizations should implement a cybersecurity plan that effectively combines technology, personnel, and regulatory oversight to avoid future disruptions.

Software Validation and Testing- A secure environment is built on the foundation of safe and dependable software updates. The industry has widely accepted the practice of prolonged beta testing for software updates. Implementing more stringent validation procedures for updates to prevent the deployment of untested patches that could result in system-wide failures.

- Testing in a simulated environment that replicates real-world conditions is essential for deployment.
- The implementation of staggered release mechanisms aims to reduce the impact of faulty updates on a smaller area.

These practices ensure that changes do not lead to critical failures during live operations [1],[2].

Defense Architecture- Implementing a multi-faceted defense strategy, incorporating various components such as endpoints, networks, identities, and cloud infrastructure, can ensure continuity and security even if one element is compromised. The CrowdStrike incident affected millions of systems unraveling the risk of single-point security dependency. Implementing multi-vendor security solutions from various vendors, deploying intrusion detection/prevention systems, and employing zero-trust frameworks can significantly boost the resilience of IT systems [1],[3],[7].

ISSN 2581-9429 IJARSCT
DOI: 10.48175/IJARSCT-24524

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, March 2025
Impact Factor: 7.67

Incident Response and Recovery Strategies- During the 2024 CrowdStrike incident, several organizations faced difficulties due to lack of automated recovery software.

- Multi disciplinary incident response teams
- Implement robust patch management process
- Organizations should carry out frequent crisis simulations to assess their readiness in authentic scenarios

Real-Time Surveillance and Threat Intelligence- Continuous system monitoring is essential for detecting abnormalities. After the 2024 incident, CrowdStrike upgraded its real-time monitoring and anomaly detection capabilities using machine learning and behavioral analysis. Organizations can detect system irregularities, reduce false alarms, and respond quickly to emerging issues by integrating Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) [1][8].

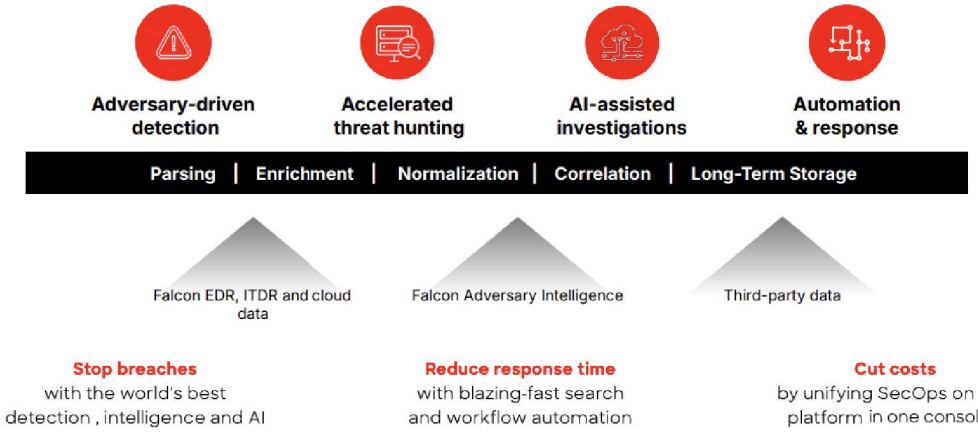

Fig. 3. CrowdStrike Falcon Next-Gen SIEM (Accessed from: https://assets.crowdstrike.com/is/content/crowdstrikeinc/unlock-soc-transformation-white-paperpdf)

Accountability, Governance, and External Oversight Procedures- Effective governance frameworks establish cybersecurity as an organizational predominance. The CrowdStrike incident highlighted the significance of independent code reviews and risk assessments conducted by third-party vendors. International standards such as NIST SP 800-53 and ISO/IEC 27001 offer guidance on implementing and conducting audits of secure software development practices [9],[10].

Cybersecurity Culture and Employee education- Despite the presence of advanced technology, human mistake continues to be a major point of concern. Organizations should cultivate a culture that prioritizes cybersecurity. This can be facilitated through ongoing employee training, phishing simulations and empowering employees to report cybersecurity incidents. An informed workforce can play a crucial role in identifying early signs of problems before they escalate.

Fault Isolation and Self-Healing Mechanisms in EDR

Modern EDR systems must be designed with fault isolation and self-recovery capabilities to prevent widespread disruption from internal failures. The 2024 CrowdStrike outage highlighted the risk of tightly coupled system components, where a single faulty update triggered global crashes. To avoid this, future EDR architectures should separate critical functions into modular components with limited privileges. Incorporating self-healing features—such as automated rollback, crash loop detection, and watchdog monitoring—can enable endpoints to recover independently without external intervention. These mechanisms improve reliability, reduce downtime, and help ensure that security tools do not become points of failure themselves.

ISSN 2581-9429 IJARSCT
DOI: 10.48175/IJARSCT-24524

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, March 2025
Impact Factor: 7.67

Fig. 4. Cybersecurity Strategies (Accessed from: https://wjaets.com/sites/default/files/WJAETS-2024-0473.pdf)

V. CONCLUSION

The 2024 CrowdStrike outage highlights the vulnerability of even highly secured systems when they are not adequately maintained. A routine software update rapidly spiraled into a worldwide IT crisis, impacting businesses, governments, and critical infrastructure. This incident has highlighted vulnerabilities in automated security update systems, emphasizing the need for more rigorous testing, phased deployment strategies, and fail-safe recovery procedures. The research highlighted the risks of placing too much trust in a single security vendor, thereby emphasizing the need for diversification within cybersecurity protocols.

CrowdStrike and other industry leaders made substantial improvements to update validation, enhance rollback capabilities, and integrate AI driven monitoring to identify anomalies before they result in widespread disruptions. Organizations have also re-examined their cyber resilience strategies to guarantee they have contingency security protocols in place to mitigate potential future system failures.

This incident has served as a learning experience highlighting the fine line between ensuring security and maintaining operational stability. The future of Cybersecurity should prioritize establishing trust, transparency, and developing systems capable of withstanding internal and external threats. The industry can benefit from such an event to build a more robust and adaptive security framework, thereby preventing defensive strategies from inadvertently triggering a crisis.

REFERENCES

[1]. P. Banerjee, "CrowdStrike Cyber Incident vs. Past Major Cyber Incidents: Analysis and Solutions," International Journal of Future Machine Research (IJFMR), vol. 6, no. 4, Aug. 2024. DOI: 10.36948/ijfmr.2024.v06i04.25310.

DOI: 10.48175/IJARSCT-24524

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, March 2025
Impact Factor: 7.67

[2]. O. Ogundipe and T. Aweto, "The shaky foundation of global technology: A case study of the 2024 CrowdStrike outage," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 5, no. 5, pp. 106–108, Sep.-Oct. 2024. ISSN: 2582-7138.

[3]. S. M. Kerner, "CrowdStrike outage explained: What caused it and what's next," TechTarget, Oct. 29, 2024. [Online]. Available: https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next

[4]. "CrowdStrike Expands Threat Intelligence Integration with Falcon X Premium," Nomios News & Blog, Aug. 8, 2018. [Online]. Available: https://www.nomios.com/news-blog/crowdstrike-expands-threat-intelligence-integration-with-falcon-x-premium/

[5]. CrowdStrike, "CrowdStrike Falcon® Adversary OverWatch," [Online]. Available: https://www.crowdstrike.com/en-us/resources/data-sheets/crowdstrike-falcon-adversary-overwatch/.

[6]. E. Kovacs, "CrowdStrike Faces Lawsuits From Customers, Investors," SecurityWeek, Jul. 31, 2024. [Online]. Available: https://www.securityweek.com/crowdstrike-faces-lawsuits-from-customers-investors/

[7]. S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, Aug. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207.

[8]. CrowdStrike, "The Complete Guide to Next-Gen SIEM," 2024. [Online]. Available: https://go.crowdstrike.com/definitive-guide-to-next-gen-siem-ebook-2024.html.

[9]. J. Lubell, "Integrating top-down and bottom-up cybersecurity guidance using XML," Balisage Series on Markup Technologies, vol. 17, Aug. 2016. DOI: 10.4242/BalisageVol17.Lubell01.

[10]. F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," Sustainability, vol. 15, no. 7, p. 5828, 2023. DOI: 10.3390/su15075828

ISSN 2581-9429 IJARSCT

DOI: 10.48175/IJARSCT-24524