THE CYBER EXPRESS

BY CYBLE.

EDITION 19 | SEPTEMBER 2024

Contents

FROM THE EDITOR'S DESK

AUGUSTIN KURIAN

Editor-in-Chief

Dear Readers,

Welcome to the September issue of The Cyber Express. This month, we focus on a critical concern: the escalating threat of cyberattacks on our most vital infrastructure. This is not just a technical issue but a looming crisis that could disrupt the very foundations of our societies.

The current state of cybersecurity for critical infrastructure is fragmented, with regulations and standards that fail to match the complexity of modern threats.

The voluntary norms adopted by the United Nations in 2015 have had limited impact. The International Energy Agency reports that cyber incidents targeting infrastructure have doubled between 2020 and 2022, highlighting the inadequacy of our current defenses. It's clear that a unified global cyber treaty is urgently needed—one that brings cohesion to our efforts, establishes universal standards, and fosters global cooperation.

In this issue, we feature insights from some of the most knowledgeable voices in the field. Renowned TV personality Cathy Pedrayes shares essential cyber tips for every digital user, while Dr. Sheeba Armoogum discusses the crucial relationship between cybersecurity and human behavior. Matthew Rosenquist, CISO and Cybersecurity Strategist at Mercury Risk and Compliance, Inc., offers expert guidance on fortifying critical infrastructure.

We also have thought-provoking contributions from industry leaders. Dhiraj Ranka, CISO of TATA AIG General Insurance Limited, navigates the complexities of today's cybersecurity landscape.

Dr. Mohammad Khaled, VP of Growth and Business Transformation at REACH Digital, emphasizes the importance of protecting AI systems and data. Jane Teh, Senior Director of Security Consulting Services at vCyberiz, explores how artificial intelligence is playing a pivotal role in data protection and leakage prevention.

Prianshu Khandwala, CISO at Sun Pharma, discusses the power of AI and cybersecurity in safeguarding pharmaceutical intellectual property. Amit Joshi, CISO at Adani Cement, examines evolving strategies and regulations in the digital age.

Vishal Salvi, CEO of Quick Heal Technologies Limited, dissects the recent CrowdStrike crash, offering a broader analysis of its implications. Apu Pavithran, CEO and Founder of Hexnode, highlights the ransomware strikes on Britain's NHS and questions whether healthcare is truly prepared. Finally, Mel Migrino, SEA Regional Director at Gogolook, explores AI governance as a crucial business enabler.

This issue is more than a collection of insights; it is a call to action. Protecting the infrastructure that supports our daily lives is essential. As we advance in the digital age, our strategies must be robust, unified, and forward-thinking.

We hope you find this issue both insightful and essential. Your feedback is invaluable as we navigate these challenges together, and we invite you to share your thoughts with us at **editorial@thecyberexpress.com**. .

Stay informed, stay secure.

Augustin Kurian
Editor-in-Chief
The Cyber Express

STAFF

Editorial

Augustin Kurian
Editor-in-Chief
editor@thecyberexpress.com

Paul Shread
International Editor
paul.shread@thecyberexpress.com

Krishna Murthy
Deputy Editor
krishna.murthy@thecyberexpress.com

Avantika Chopra
Associate Editor
avantika@thecyberexpress.com

Samiksha Jain
Magazine Producer
samiksha.jain@thecyberexpress.com

Mihir Bagwe
Principal Correspondent
mihir.bagwe@thecyberexpress.com

Ashish Khaitan
Correspondent
ashish@thecyberexpress.com

Alan Joseph
Technical Writer
alan.joseph@cyble.com

Management

Rajashakher Intha
Director of Marketing
And Product Management
raj@thecyberexpress.com

Ashish Jaiswal
Conference Manager
ashish.j@thecyberexpress.com

Anees Shaik
Sponsorship Sales Manager
anees.shaik@thecyberexpress.com

Priti Chaubey
Manager - Communications
priti.c@thecyberexpress.com

Pallavi Dash
Social Media Manager
pallavi.dash@thecyberexpress.com

Ravi Gupta
SEO Analyst
ravi@thecyberexpress.com

Vittal Chowdry
Design Lead
vittal@thecyberexpress.com

Some of the Images in this magazine are provided by ***Freepik***

Image credits: Shutterstock & Freepik

THE GREAT CROWDSTRIKE CRASH: A MULTIFACETED EXAMINATION

- By Vishal Salvi

Chief Executive Officer,
Quick Heal Technologies Limited

On July 19, 2024, the world witnessed a widespread computer outage caused by a faulty update from cybersecurity firm CrowdStrike. This event -- dubbed the Great CrowdStrike Crash -- had a ripple effect across industries, highlighting vulnerabilities and sparking discussions on various aspects of cybersecurity.

This essay will delve into this incident, exploring its technical cause, global impact, the lingering questions in the aftermath, and most importantly the different perspectives on this issue.

But let's start at the top…

From a technical standpoint, the culprit was a defective update for CrowdStrike's Falcon Sensor software. This software, designed to protect Windows systems, contained a bug that triggered critical errors that led to the dreaded Blue Screen of Death (BSOD) system crashes, with swift and severe ramifications for businesses, hospitals, and even emergency services that found themselves crippled as countless devices became inoperable.

This begs the question though, why would one bug cause such a devastating impact across the globe? There are two fundamental reasons

1. CrowdStrike is a leader in the EDR (End point Detection and Response) market and the scope of this update was exponentially large

2. These were not any ordinary software updates; these updates caused their driver to malfunction leading to the system crash. The drivers run in privilege mode and if not written/configured/input properly can lead to a computer crash.

The global impact of the crash was undeniable. Financial institutions, airports, and media outlets all reported disruptions. The interconnected nature of modern society meant that a problem in one sector can cascade outwards, causing widespread chaos.

Crowdstrike estimated that around 8.5 million devices were impacted, and though it might be too early to put a dollar value on the outage, CNN reported that its impact might have touched $1 billion already.

While India largely escaped the financial sector meltdown seen elsewhere, the crash still managed to disrupt various parts of the Indian business landscape, highlighting vulnerabilities and raising important questions. One of the most immediate effects was felt in the Indian IT sector. Several brokerage firms, including Nuvama,5paisa, Angel One, IIFL Securities and Motilal Oswal, reported disruptions to their operations.

The crash also shone a light on the potential vulnerabilities of critical infrastructure in India. News reports suggest that even major airports like Delhi's Indira Gandhi International Airport experienced disruptions. This highlights the need for Indian companies and government agencies to diversify their tech stack and implement robust backup systems to minimize downtime during such global outages.

For a global disruption like this, there are bound to be many conspiracy theories. There are articles which speculate that this was a planned sabotage and its impossible for a company like CrowdStrike to not perform a basic check like this before releasing this content update in production.

I would recommend we wait for a proper root cause analysis before we jump to any conclusions, CrowdStrike's official statement does not point to any sabotage or unauthorized change. In the coming days more details will emerge on what was the real miss so that we all can learn from this.

In the aftermath, CrowdStrike issued a public apology and scrambled to contain the damage. They quickly identified the buggy update and rolled out a fix, but for many affected systems recovery was a manual and laborious process.

The road to recovery…

As I write this, I am aware there are still many organizations which are trying to recover completely from this incident. The world that we live in today is deeply dispersed when it comes to computers and communications among them, with IT support being mostly remote.

The nature of this incident is such that it needs local intervention because systems have crashed and hence no longer communicating on the network. So, your IT support staff will have to help you navigate over call and also share recovery keys and admin passwords that are no longer available to end users.

Several server farms in data centers have crashed and they will need to be brought up one by one. This is a time-consuming activity and although the recovery is pretty straightforward, because of the manual nature of this recovery, it will take time and lots of manhours to get all operations back to normal.

Beyond the technical aspects, the crash sparked discussions on the broader cybersecurity landscape. It highlighted the delicate balance between robust security and the potential for unintended disruption. Security software, while crucial for defence, can also introduce vulnerabilities if not rigorously tested and implemented.

The incident also outlined the need for robust communication channels between cybersecurity vendors and their clients. Timely updates and clear instructions during outages are essential for minimizing downtime and ensuring a swift recovery. Luckily in this case, the identification of the issue and remediation steps were quickly available.

This is not the first time that such an issue has happened, however the scale and impact of this one is unparalleled. This is also a result of the way the modern world is powered by digital infrastructure and the role cybersecurity plays in it. It's dangerously complex where we are constantly fighting against the bad guys and striving to stay one step ahead of them.

There is a gold rush to hunt for new zero days (vulnerabilities that are as yet unknown) so that new forms of attacks can be developed and launched. Security firms, hence, have to get it right all the time while balancing quality and security.

The Great CrowdStrike Crash serves as a cautionary tale for the cybersecurity industry. It emphasizes the importance of thorough testing, clear communication, and a proactive approach to risk management. As we rely more heavily on technology, ensuring its stability and security becomes paramount. The lessons learned from this incident can help us build more resilient systems and prevent similar disruptions in the future. This incident served as a stark reminder of our dependence on technology and the potential consequences of even minor software glitches.

About Author:

Vishal Salvi is the CEO of Quick Heal Technologies Ltd., with nearly three decades of experience in IT and cybersecurity. He is passionate about innovation, cybersecurity awareness, and mentoring future professionals, dedicated to making cyber safety a fundamental right and driving digital security advancements on a global scale.


THE CYBER EXPRESS
SCAN AND STAY UPDATED WITH
REAL TIME CYBERSECURITY NEWS
To advertise with us, write to: marketing@thecyberexpress.com