Microsoft-CrowdStrike outage: How a single software update was able to cause IT chaos across the globe

July 22 2024, by Feng Li

Credit: Pixabay/CC0 Public Domain

The world as we know it increasingly relies on digital connectivity that, for the most part, works quietly and invisibly in the background. So how did a single software update bring down half the internet?

The global IT outage on 19 July serves as a stark reminder of our vulnerability to technological failures. Triggered by a single faulty software update provided by the cybersecurity firm, CrowdStrike, this had a disastrous impact on airlines, media outlets, banks, and retailers worldwide, particularly businesses that use Microsoft Windows operating systems.

This incident, described as the "largest IT outage in history," reminds us of the extensive web of IT interconnections that sustain our digital infrastructure—and of the potential for far-reaching consequences when something goes wrong.

What started with delays at airports turned into widespread flight cancellations. The disruption in airline systems doesn't just disrupt flight schedules, it also affected global supply chains reliant on air cargo, demonstrating the multifaceted nature of modern IT ecosystems. Meanwhile, broadcasts were interrupted at numerous TV and radio stations and operations at supermarkets and banks were brought to a standstill.

Preliminary analyses suggests the chaos stemmed from a software update from CrowdStrike's Falcon Sensor security software that was applied to Microsoft Windows operating systems. Workers in companies using CrowdStrike were met with the "blue screen of death" (a screen with an error message indicating a systems crash) when they tried to log in.

In addition to exposing the hidden web of dependencies that sustain our digital society and economy, the outage also highlighted the geopolitical dimensions of these dependencies. Countries with strong ties to Microsoft and CrowdStrike felt the brunt of the impact, but businesses in countries like China, with their relatively insulated and controlled IT infrastructures, appear to have been less affected.

With growing geopolitical tensions in recent years, China and a growing number of other countries have actively developed their own cybersecurity measures and digital infrastructures, which may have mitigated the effects of this incident.

China's focus on using indigenous technology and reducing their dependency on foreign technology may have also contributed to the lesser impact on their systems. The incident serves as a stark reminder that technological dependencies can translate into geopolitical vulnerabilities, with state authorities increasingly needing to consider not just the economic but also the strategic and geopolitical implications of their IT alliances.

Recovery and implications

How the affected sectors have managed this crisis reflects both the strength and vulnerabilities of their own security and disaster recovery strategies. The primary issue has been identified and reportedly rectified. The slow recovery process ahead will show the significant challenges to come in restoring service continuity within our complex, deeply interconnected digital ecosystems.

It's particularly surprising that despite numerous past lessons, like the TSB IT migration disaster in 2018 that affected millions of customers of the UK bank, a staggered software rollout was not employed.

The absence of this step, a fundamental yet critical strategy in IT management, exposed the fragility of systems that many presumed robust. It has also raised serious questions about the resilience of both the Windows operating systems and the cybersecurity measures by CrowdStrike that are supposed to protect them.

In addition, the episode highlighted the strategic risks of relying on a

single source of technology. This global outage showed how important it is to have diverse technological alliances to enhance national security and economic stability, while raising concerns about the potential for hostile states to exploit such vulnerabilities. This incident will add a new layer of urgency to international cybersecurity collaborations and policy interventions.

As services begin to stabilize and resume, this outage should serve as a wake-up call for IT professionals, business leaders, and policymakers alike. The pressing need to reassess and even overhaul existing cybersecurity strategies and IT management practices is clear. Improving system resilience to withstand large scale disruptions must be a priority.

The global IT outage marks a timely reminder and a critical juncture for discussions on digital resilience and the future of technology governance at the business, infrastructure and policy levels.

What about AI?

Something else we don't know the answer to yet is this: if a single software bug can take down airlines, banks, retailers, media outlets and more around the world, are our systems ready for AI?

Perhaps we need to invest more in improving software reliability and methodology, rather than rushing out chatbots. An unregulated AI industry is going to be a recipe for disaster, particularly in a world with growing geopolitical tensions.

While it's essential to embrace emerging technologies like AI or blockchain, we must also get the basics right. Cybersecurity operators need to ensure that fundamental IT management and maintenance practices are strong and reliable, and able to handle anything from a cybersecurity attack to a simple software update.

The lessons learned from this incident will undoubtedly influence future strategies in IT infrastructure development and crisis management.

Provided by The Conversation

Citation: Microsoft-CrowdStrike outage: How a single software update was able to cause IT chaos across the globe (2024, July 22) retrieved 22 July 2024 from https://techxplore.com/news/2024-07-microsoft-crowdstrike-outage-software-chaos.html