TechXplore

From ATMs to flights, epic IT crash leaves trail of destruction

July 22 2024, by Amy Thomson, Shona Ghosh, Vlad Savov, Bloomberg News

Credit: Unsplash/CC0 Public Domain

In what will go down as the most spectacular IT failure the world has ever seen, a botched software update from cybersecurity firm

CrowdStrike Holdings Inc. crashed countless Microsoft Windows computer systems around the world on July 19.

Microsoft Corp. and CrowdStrike have rolled out fixes, and systems are gradually being restored. But for several hours, bankers in Hong Kong, doctors in the UK and emergency responders in New Hampshire found themselves locked out of programs critical to keeping their operations afloat. Some businesses are facing the prospect of continued disruptions as the restoration process is, in some cases, requiring tech workers to manually reboot systems and remove faulty files.

"This is unprecedented," said Alan Woodward, professor of cybersecurity at Surrey University. "The economic impact is going to be huge."

The catastrophic failure underscores an increasingly dire threat to global supply chains: The IT systems of some of the world's biggest and most critical industries have grown heavily dependent on a handful of relatively obscure software vendors, which are now emerging as single points of failure. In recent months, hackers have exploited this phenomenon, targeting vendors to bring down entire sectors and governments.

Adding to the disruption, Microsoft experienced a separate and apparently unrelated problem with its Azure cloud service on Thursday that lasted for several hours. On Friday afternoon, the company said in a post on X that all Microsoft 365 apps and services had been restored.

By Friday morning in New York, many systems were coming back online.

CrowdStrike Chief Executive Officer George Kurtz said in a pre-6 a.m. post on X that the fault had been identified and the company had deployed a "fix." It requires rebooting Windows machines and removing bad files, a very manual process typically performed by information technology professionals with administrative permissions. Many of those IT specialists faced challenges in carrying out those tasks remotely while Windows was crashing.

Shares of CrowdStrike dropped 11% to $304.96 in New York trading, wiping out more than $9 billion in market value. It was their biggest single-day decline since November 2022. Microsoft shares fell less than 1% to $437.11.

There have been outages before, but none that approached the scale of CrowdStrike's, which hit airlines, banks and health-care systems, and whose repercussions are still being felt. In 2017, a series of errors within Amazon.com Inc.'s cloud service affected the operation of tens of thousands of websites. In 2021, issues at content delivery network Fastly Inc. took out the websites of several media networks, including Bloomberg News. Disruptions also incapacitated Amazon's AWS cloud service.

"This will be the largest IT outage in history," said Troy Hunt, an Australian security consultant and creator of the hack-checking website Have I Been Pwned. "We're really only starting to see the tip of the iceberg."

As businesses work to restore their systems, meanwhile, hackers have already found an opportunity for scams in the form of hastily created websites that claim to offer restoration services for machines brought down by the CrowdStrike crash.

Airlines

Airport hubs from Berlin to Delhi struggled with delays, cancellations and stranded passengers at a time that was already particularly busy for travel. FlightAware said more than 21,000 flights were slowed globally, and travel disruptions were expected to stretch into the coming days.

United Airlines Holdings Inc. and Delta Air Lines Inc. gradually resumed operations on Friday. Other U.S. carriers that had temporarily grounded flights included American Airlines Group Inc. and Spirit Airlines Inc., according to the Federal Aviation Administration.

Finance

The London Stock Exchange Group has resolved an issue that stopped the bourse from publishing news on its website via RNS, a service that publicly traded companies use to distribute price-sensitive regulatory announcements.

A number of financial institutions were forced to revert to backup systems during the IT failure. Bankers at JPMorgan Chase & Co., Nomura Holdings Inc. and Bank of America Corp. were unable to log on for part of the day on Friday, and the trading desk at Haitong Securities Co. was out of action for about three hours.

Thousands of JPMorgan Chase ATMs were down as well due to the CrowdStrike crash, Bloomberg reported. Some teller stations also weren't working. The majority of the bank's ATMs were operational as of late Friday in the U.S., according to a person familiar with the matter who asked not to be identified because the details haven't been publicly disclosed.

Health

The disruptions also impacted critical infrastructure, including emergency services.

Doctors at the UK's National Health Service couldn't access scans, blood tests and patient histories. Memorial Sloan Kettering Cancer Center in New York and Boston-based Mass General Brigham warned that the CrowdStrike issue was affecting patient care. Hospitals in Europe reported having to close clinics and cancel procedures.

New York's 911 and emergency systems were also impacted. New Hampshire's emergency 911 services are functioning again after a failure in which operators could see calls coming in but couldn't answer them.

Automakers

Renault was forced to halt production in the afternoon at its Maubeuge plant (on the Kangoo production line) and also at its Douai plant for lack of parts as suppliers got hit by the outage.

Tesla Inc. Chief Executive Officer Elon Musk said on Friday that he has stopped using CrowdStrike software. "We just deleted CrowdStrike from all our systems," Musk said in a post on his social media site X. He previously said that the outage "gave a seizure to the automotive supply chain."

Musk didn't specify whether all of his companies were dropping CrowdStrike's software. In addition to Tesla and X, his business empire includes Space Exploration Technologies Corp. and startups such as Neuralink Corp. and xAI Corp. Musk didn't immediately respond to a request for comment.

Government Agencies

The most significant impacts in the U.S. are to health care, state and local police, plus some Department of Energy sites and the .gov domain, according to a person familiar with the consequences of the CrowdStrike outages on US government systems.

The National Security Council has held multiple calls, including with agencies across the US government. The Cybersecurity and Infrastructure Security Agency convened a call across sector-coordinating councils. The Department of Energy and the Department of Health and Human Services have also been talking to their sectors.

Airlines and airports are now functional, and banks to a large extent too, the person said.

2024 Bloomberg L.P. Distributed by Tribune Content Agency, LLC.

Citation: From ATMs to flights, epic IT crash leaves trail of destruction (2024, July 22) retrieved 22 July 2024 from https://techxplore.com/news/2024-07-atms-flights-epic-trail-destruction.html