Amazon crash is only the beginning - Nobody but FOOLS use networks

By HARRIET ALEXANDER,

It was shortly after 8am in **London** when the **British government**'s websites began to flicker and fade.

Most of America was asleep, but a few night owls on the East Coast found their Disney streaming services stall.

Those calling Lyfts to get home from a Sunday night party were struggling. Routine activities were grinding to a halt.

As the eastern United States awoke, the scale of the problem became clear.

United Airlines and Delta found their passengers could not use online services. Commuters accustomed to scanning the **New York Times**' morning newsletter went without. Snapchatters fell silent; **Reddit** forums were hushed.

One third of all online users worldwide interact with Amazon Web Services (AWS) daily, according to DeepField Networks: companies ranging from **Venmo** to Reddit to Ring all rely on AWS servers. And, on Monday morning, the system was down - **crashing a significant portion of the internet**.

The fact such an outage could happen at all is 'surprising,' said cybersecurity expert James Knight, senior principal at **Digital Warfare**, which helps companies identify and shore up online vulnerabilities. It is also a troubling indicator of a new brand of chaos from which none of us are immune.

Knight told the Daily Mail: 'My first thought was wondering how it could occur. Apparently, some sort of database went down.

+4

View gallery

One third of all online users worldwide interact with Amazon Web Services (AWS) daily, according to DeepField Networks: companies ranging from Venmo to Reddit to Ring all rely on AWS servers. And, on Monday morning, the system was down

TRENDING

'It's surprising that one thing affected their network, because usually there's backup, and redundant systems all running at the same time. One particular system going down is very, very surprising.'

Knight admitted he was puzzled by the outage which, he noted, will have cost Amazon hundreds of millions of dollars.

It began at 3:11am ET. By 5:01am ET the problem had been identified, and a 'fix' deployed within 20 minutes.

Yet it remained unresolved and, at 8:48am ET, Amazon issued another update saying further fixes were being carried out.

The specter of a cyber-attack has inevitably been raised but, according to Knight, this is unlikely.

He explained: 'A cyber professional like myself, or whoever is currently looking at it, would be able to see if it were a hack. It's called an indication of compromise, an IOC.

'We'd see maybe a malware signature; some sort of unauthorized access; something in the logs showing that there's some sort of access gained, or some anomalous traffic. There's nothing to indicate that here.'

What's more, he said, Amazon is legally required to disclose any hack.

Instead, the company has said that the problem derived from their site in Virginia, known as the US-EAST-1 Region.

Their last big outage was in 2021 - a sign, Knight said, of the actual resilience of AWS's systems. But problems, when they happen, can be devastating.

In July 2024 cybersecurity company CrowdStrike went down for several days, causing the largest-ever IT outage in history.

The glitch itself only lasted for 90 minutes, but it took some companies days to recover. One insurer calculated that the issue cost Fortune 500 businesses alone more than $5 billion in direct losses, with airlines and hospitals hardest hit.

Telecoms company AT&T found its network unavailable several times last year, with a particularly damaging 11-hour meltdown in February.

Knight said it is a sign of the times, and something we simply have to learn to live with.

+4

View gallery

Pictured: An Amazon Web Services data center in Virginia

Pictured: Downdetector reports of AWS outages spiked

+4

View gallery

Knight said it is a sign of the times, and something we simply have to learn to live with

'Our lives are online, and it's just going to happen,' he said. 'AWS, along with Google and Microsoft, are the gold standard in cloud computing. So it's not like AWS's rivals will be smug, because tomorrow it could happen to them.

'I can't really criticize AWS. They reacted pretty well. I don't know if anybody's head is going to roll, but it will be taken very seriously, and I think they're going to derive the lessons learned so that they can improve.'

Given the fiercely competitive cloud computing space, however, AWS will not be sharing their fixes with their rivals.

Does it mean that companies today have too many eggs in one basket? Should they be sprinkling their services around, using more than one cloud computing company?

Knight said they could in theory, but it would be difficult to administer, and not necessarily helpful.

'AWS is already divided in a number of baskets, and that's why people keep things in the cloud,' he said. 'Some of their servers are in the cloud in one location and some in another location: some on the East Coast of the US, some on the West Coast, some in Asia and it is spread around.'

By 11:43am ET on Monday, over eight hours after the first sign of trouble, Amazon sounded optimistic that the end was in sight.

'We have narrowed down the source of the network connectivity issues that impacted AWS Services,' the company said. 'The root cause is an underlying internal subsystem responsible for monitoring the health of our network load balancers.'

They said they were deliberately slowing some services 'to aid recovery' and were still 'actively working on mitigations.'

Knight said Amazon would be studying in detail what went wrong and learning lessons from the outage.

'They're going to determine the root cause,' he said. 'And then they're going to improve their procedures.'

They'll 'come out stronger for it,' he said, and they will do whatever they can to ensure that it doesn't happen again. But the truth, that we will all have to live with is, it will. And next time it could be even worse.