A global IT outage brought supply chains to their knees—we need to be better prepared next time

July 25 2024, by Sanjoy Paul and Towfique Rahman

Credit: CC0 Public Domain

Friday's global IT outage—caused by a faulty software update from cybersecurity firm Crowdstrike—wrought havoc on business operations around the world.

Severe disruptions were reported in multiple countries, including Australia, New Zealand, Japan, India, the United States and the United Kingdom. Many businesses were unable to access critical systems and data, leading to significant delays and financial losses.

As the crisis struck, many of us would have been preoccupied with its immediate consumer impacts—hospital systems going down, some supermarkets operating cash-only, flights getting delayed, and news anchors reading from printed notes.

But it's often forgotten that our supply chains—the complex networks that turn raw materials into finished products and get them where they're needed—have also become deeply integrated with technology. They were hit hard too.

Over the past few decades, advanced IT systems have been adopted in supply chains to better manage inventory, coordinate shipping and logistics, make decisions and share information.

This technology has brought enormous benefits to supply chain management. But it has also introduced major new vulnerabilities, as we've just seen first hand. We need to be better prepared to face similar crises in future.

Supply chains depend on technology

Advanced IT systems now enable real-time tracking, automated inventory management, and seamless communication across global supply chains. This has made them more efficient, transparent and responsive.

But to achieve such precision and speed, they've also become highly interdependent. Making supply chains operate efficiently hinges on the

timely success of everyone—and all the technology—involved.

We've now seen just how quickly things can come undone.

Transport systems in particular were [hit hard](). In the wake of the outage, both [shipping companies]() and [ports]() reported disruptions.

Many people have been directly affected by canceled or delayed passenger flights. But Delivery firm Parcelhero has [warned]() there could also be significant ripple effects for air freight:

"Not only will slots for dedicated airfreight flights be disrupted, but many international goods and packages are transported not only in specially designed cargo planes but also in the cargo holds of passenger aircraft."

Other air freight experts have [suggested]() a full recovery could take days or even weeks.

The finance and retail sectors also have an important role to play in supply chains, and faced their own disruptions.

Many Australian banks faced [outages](), as did major accounting software providers myob and Xero. Many retail operations, particularly those with extensive e-commerce platforms, saw customers face delays in order processing and delivery.

Some further impacts of the outage may not be visible immediately. We'll only be able to see them as they propagate through supply chains over time.

How can companies be better prepared?

Any one of these disruptions in isolation would have been a significant incident. For them all to happen at once made Friday's crisis strikingly rare. That doesn't mean businesses shouldn't be prepared. The question is when, not if, the next global IT outage will occur.

The nature of Friday's outage made its impacts difficult to avoid. But not all IT threats are the same. To build more resilient supply chains, businesses within them need to have robust contingency plans in place—even if it means maintaining the ability to perform key processes manually and use paper records (as many did on Friday).

One strategy is for businesses to diversify their sources of key software and technology. This helps avoid over-reliance on what might become a single point of failure. Risks should be monitored proactively, with regular stress tests and audits.

Investing in cybersecurity measures can also often prevent and minimize the impact of many IT threats. This includes regularly updating software, training staff on best practices and employing relevant advanced security technologies.

Educating staff on identifying and responding to potential IT issues is also crucial to reducing human error. There also need to be clear communication channels in place during outages to maintain transparency and trust. These protocols should be updated regularly.

Don't put all your eggs in one basket

One of the biggest things to account for in supply chain management is the risk a single "link" breaks—perhaps a key supplier becomes unable to produce a particular input, or it can't be transported in time.

On top of diversifying the software systems used for key tasks,

businesses should also diversify their sources of key inputs and logistics needs.

Diversifying suppliers mitigates the risk of depending on a single source and means a business has alternative options. Ideally, this allows it to continue operations relatively smoothly when supply is disrupted.

Bringing manufacturing and logistics onshore or to a nearby country (nearshoring) can also help mitigate the risks from international disruptions. And shortening the supply chain by reducing the number of middlemen can reduce potential points of failure.

Recovering quickly is important

How quickly a supply chain can recover from an IT outage or other crisis depends on its preparedness and resilience. Many of the strategies we've discussed can significantly reduce recovery times and minimize operational disruptions, allowing businesses to get back to normal.

New technologies have been a boon for supply chain management, but they have also added huge new vulnerabilities. Taking a proactive approach to cybersecurity and contingency planning can't prevent all disasters, but it remains a business' best bet.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation