Has the cyberattack on DP World put Australia's trade at risk? Probably not—this time

November 13 2023, by Flavio Macau and Paul Haskell-Dowland

Credit: CC0 Public Domain

Australians getting ready for Christmas this week had reason to believe even the best of preparations were not enough after a cyberattack hit all

its major ports.

DP World, which operates container ports in Australia and the region, first detected problems last Friday so unplugged its systems to minimize the impact while it examined what had happened.

While operations resumed at the ports Monday, the cause is still unclear and the incident continues to be investigated.

With responsibility for about 40% of freight movement at Australian ports, and a significant 10% of global trade through its international operations, the attack disrupted the flow of goods coming from ports DP World operates.

Deliveries of import items such as videogames, air-conditioners, furniture and pharmaceuticals were held up.

As well, Australian exports of goods including processed meat, dairy products and fruits, all with limited shelf life, were delayed.

Why this cyber attack is significant

While DP World seems to be recovering, the incident highlights the potential vulnerability of global networks.

Supply chains rely on fully integrated solutions, from sellers overseas to buyers in Australia, to work efficiently. Information technology is embedded into them through equipment automation and data processing. Product visibility, customs clearance and checks for biosecurity risks rely on cargo information detailing where goods come from, who is responsible for them and their trading value.

With sensitive data linked to the movement of containers, it is no

wonder logistics professionals recognize cybersecurity as a major threat to operations—not to mention their obligations under the Security of Critical Infrastructure Act.

If there is still no certainty of the specific nature of the incident with DP World, there are few likely causes.

Ransomware has been on the rise, with incidents aligned to prolific cyber-criminal gangs including REVil and more recently LockBit.

In an attack, data is usually extracted from an organization and then rendered inaccessible to users—typically using encryption. The organization will usually receive a ransom demand to "unlock" the data, often payable using a crypto-currency.

In recent years the trend of double-extortion has become common, where the criminals incentivize their victims to pay by threatening to release the data publicly if they refuse.

While refusal is a possibility, the nature of the disruption could mean a loss of access to critical systems and information. If data is inaccessible, operations would need to be halted, leading to even greater losses.

Recovering systems would require restoration from backups and a thorough inspection for any traces of the original infection or compromise. Finally, checks would be needed to ensure no data had been lost and to identify any missing consignment data after the previous backup had taken place.

If the incident is a direct cyber-attack that infiltrated systems and stole or modified data, this would also require a complete system shutdown. Without the integrity of systems, consignment data cannot be trusted and the Australian Border Force would be unable to verify the content of

shipments. There would also be issues with the collection of duties, taxes and fees.

Disconnecting DP World from networks allowed the investigating team to inspect systems to look for impacted systems and to evaluate the depth of any infection. This process also needs to consider the original infection mechanism—you don't want the systems re-infected.

The timing could have been worse

The cyberattack caused the ports operated by DP World to start filling up with containers, but it had not yet become critical.

While Black Friday, Cyber Monday and Christmas are an extra busy time for retailers, there is usually a marginal increase in movement compared to other times of the year, typically less than 10%. With around 1.4 million containers to be moved in the last three months of the year, the impact of losing a few days should be minimal.

Big retailers typically start making orders for Christmas in August, with deliveries starting as early as October. While they keep inventory in check, it is unlikely that operations work in just-in-time mode.

Especially in Australia, where the distance from major global flows, the lack of alternatives such as railroad imports and lessons learned from COVID has bred risk averse businesses that are extra cautious to avoid empty shelves.

Also, ports can quickly recover. When container volumes go up, extra labor and equipment can be organized to increase the output of a terminal. In the last three years the number of time slots used by trucks has seldom reached 90% of total availability.

DP World should quickly be able to resolve any backlogs arising from this incident.

The hidden problem behind this attack

A problem for Australia is the potential effect of the cyberattack on its reputation as a shipping destination. When port facilities fill up with containers to the point where ships are delayed, costs quickly escalate to millions of dollars.

And numbers haven't been shiny lately.

The Maritime Waterline 69 report shows ship turnaround time increased from 35 hours early in 2020 to more than 50 hours in 2022. Port congestion went from a little over 10% of ships waiting for more than two hours to over 22%. And average waiting time at anchorage went up from 17.3 hours before COVID to 126.5 hours in mid-2022.

Add the risk of cyberattacks to this and Australian ports may lose their competitiveness, with fewer companies interested in sending their ships down here—or requiring a premium price to do so.

While the DP World cyberattack is unlikely to upset Christmas, the aggregated impact such attacks could have on Australia's reputation as an important shipping hub, must be taken seriously.

Provided by The Conversation

Citation: Has the cyberattack on DP World put Australia's trade at risk? Probably not—this time