Waterstons
we're with you

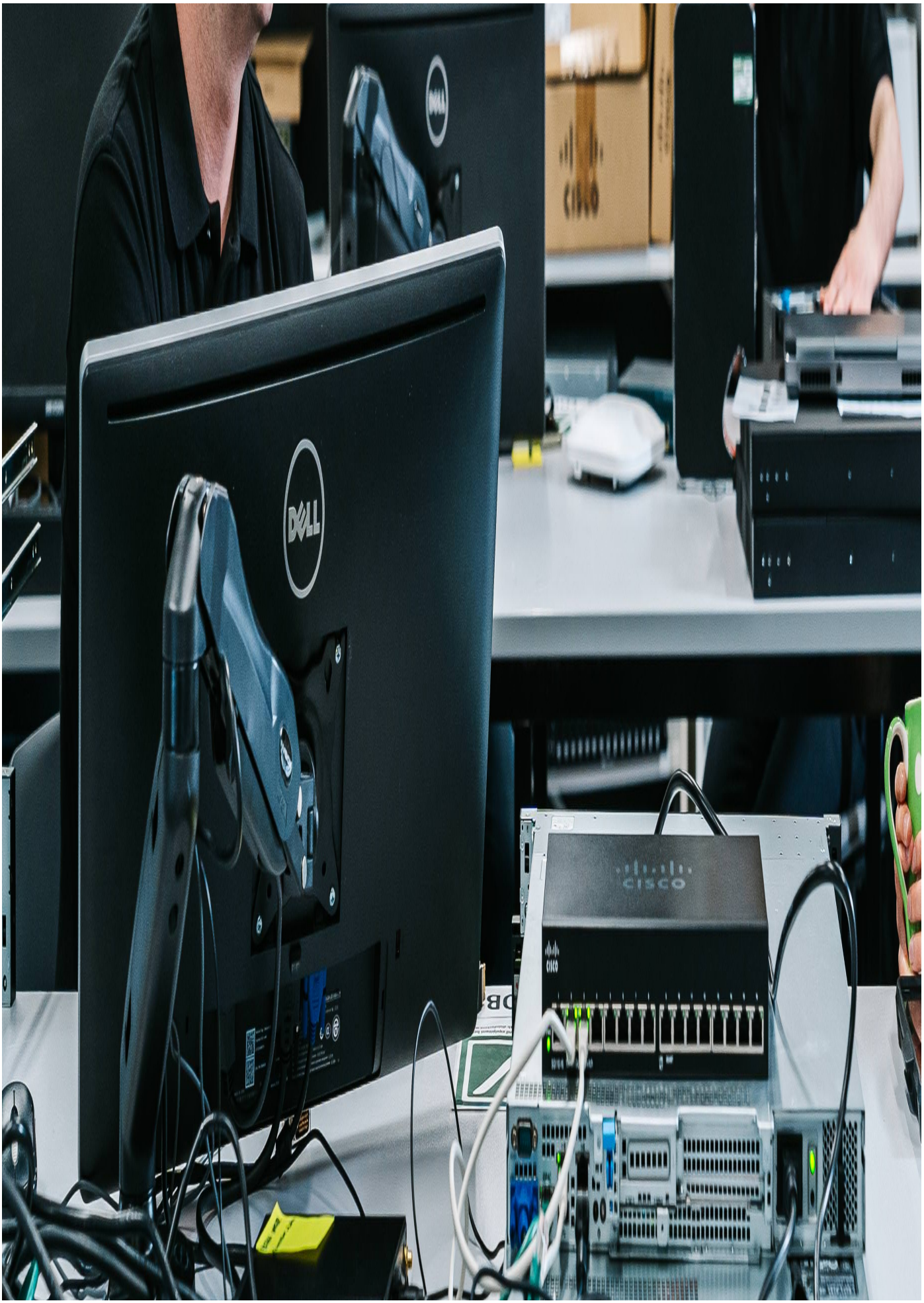
+44 345 094 0945
www.waterstons.com

News article

Dec 2023

Cyber Incident Review

DP World Australia's port operations hit by cyber attack. Read about it here and how your organisation to stay vigilant and protected.


DELL
cisco

A major cyber attack on Australia's biggest port operator, Dubai Ports (DP) World, forced the organisation to take its IT systems offline, and shut down operations at its Sydney, Melbourne, Brisbane and Fremantle ports, leaving cargo stranded on the docks.

What Happened?

Late on Friday, November 10th, DP World detected unauthorised activity on its network. The port operator was quick to activate its incident response plan, which involved restricting landside access to ports IT systems; effectively shutting down ports in Sydney, Melbourne, Brisbane, and Fremantle.

While containers could still be unloaded from ships, trucks were unable to leave the port due to the IT shutdown, leading to a backlog of 30,000 cargo containers at the four ports. Since DP World is responsible for 40% of Australia's maritime freight, the Australian government was quick to respond, calling a meeting of the National Emergency Management Agency to deal with a 'nationally significant incident'.

After almost three days of downtime, on Monday, November 13th, DP World confirmed resuming operations at its ports after recovering key systems, however, some industry reports claimed that the Port of Sydney may not be allowing exports for several weeks, indicating that the cyber attack could have impacted some sites more severely than others. As part of the ongoing investigation into the incident, DP World has confirmed that threat actors were able to exfiltrate data from the corporate network, although there has been no confirmation of what type or volume of data was stolen.

DP World has also not yet confirmed how threat actors were able to access systems, however, experienced cyber security analysts have suggested that DP World may have been another high-profile victim of the Citrix vulnerability, after researchers identified several public-facing devices on DP World's network that were vulnerable to the Citrix Bleed vulnerability.

Wider Implications

This incident appears to be part of a growing trend of attacks on major global ports in 2023, with attacks on Portugal's largest port, the Port of Lisbon, in January, and Japan's largest port, the Port of Nagoya, in July.

The mixture of IT and Operational Technology (OT) systems in ports can make them challenging environments to secure, and the significant economic impact of even a short downtime of a port, makes them attractive targets for threat actors looking for a ransom payment, or state aligned threat actors aiming to cause significant disruption to nations supply chain. Australia in particular has faced a number of cyber attacks against Critical National Infrastructure (CNI), with the Australian Signals Directorate (ASD) annual report revealing that they had responded to 143 cyber incidents at CNI between June 2022 and June 2023, increasing from 95 incidents in the year before. This increase mirrors a similar one observed in cyber attacks on Australian organisations, with high profile attacks against Optus and Medibank triggering a review of the country's cyber security laws.

Organisations Should

• Review their network for any Citrix NetScaler ADC or Gateway devices vulnerable to the Citrix Bleed vulnerability (CVE-2023-4966) and ensure that all devices are up to date with the latest patch.

• Ensure they have implemented a patch management process that sets out the requirements for deploying patches. This should be supported by an automated patch management system which can monitor which version is being used by managed devices, and deploy patches quickly to all devices in an organisation.

• Ensure they have implemented an effective incident response plan which is regularly tested to ensure that it can be deployed quickly and effectively, to help reduce the impact and scale of potential incidents.

• If operating Operational Technology (OT), define secure network architecture principles for their OT environment to adhere to, such as network segmentation, restricted data flows, and major and minor enforcement boundaries. These principles and their implementation should be subject to a regular independent review.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430

https://waterstons.com.au/print/pdf/node/6942