CDRU
Costs Down Revenue Up

Blog

The current state of cyber-security for critical infrastructure in Australia

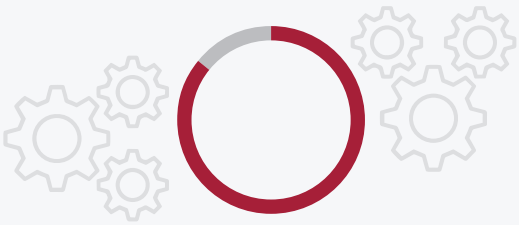
Author: Kevin Nietzke

Date: September 2021

The current state of cyber-security for critical infrastructure in Australia

In an age of rising cybercrime, no company should think it's exempt from attack.

Cybercrime has become a top concern for Governments, Enterprises and SME's around the globe. A number of massive attacks on unprepared companies have left them picking up the pieces and looking for new ways to ramp up their security.



86% of critical national infrastructure (CNI) organisations have detected cyber-attacks on their Operational Technology (OT) or Industrial Control Systems (ICS) in the last 12 months.

Source: Bridewell Consulting: CNI Cyber Report: Risk & Resilience

93% of these admit to a successful attack.

According to a recent report from independent cyber security services firm Bridewell Consulting

How do cyber-attacks manifest in real-case situations?

Americold cyber-attack (16 November 2020)

With revenue of US$1.43B, Americold is a leading provider of temperature-controlled warehousing, distribution and logistics services.

The Atlanta based company operates 183 temperature-controlled warehouses globally.

Believed to be a ransomware incident, the attack affected the company's phone systems, email, inventory management and order fulfilment, according to reports on Twitter.

Although primarily focussed on servicing the food industry, Americold has been in talks to provide temperature-controlled storage and transportation for COVID-19 vaccines.

WestRock ransomware attack (23 January 2020)

With 2020 net sales of US$17.6B, WestRock is the second largest packing company in the United States. The attached affected their Operational Technology (OT) systems, used to monitor and control their industrial operations.

In an update to the market on 5 February 2021, WestRock indicated its mill system production was 85,000 tonnes below plan as of 4 February 2021. Given WestRock's total mill system production capacity is 15.85 million tonnes (source: WestRock 2020 Annual Report), a loss of 85,000 tonnes of mill system production, represents the equivalent of almost two days of lost production across their entire network of 32 mills.

If this amount of product loss resulted in the equivalent delayed or lost sales, it would represent $94M in delayed or lost sales.

In response to this attack, WestRock proactively shut down certain systems as well as taking steps to supplement existing security monitoring, scanning and protective measures.

The Company also implemented measures, including manual processes, to respond to customers' needs. The Company is now systematically bringing its information systems back online in a controlled, phased approach.

The water treatment facility in the city of Oldsmar, Florida (5 February 2021)

The cyber-attacker gained access to the system and changed the amount of sodium hydroxide (also known as lye) from 100 parts per million to 11,100 parts per million – a dramatic and potentially dangerous increase.

Luckily, an operator witnessed this cyber-attack and immediately acted such that no tainted water was delivered to local residents.

Australia is not immune – alarmingly, cases are on the rise with serious breaches of data, privacy and security across both the Enterprise and Government sectors.

Transport for NSW joined a growing list of organisations to fall victim to the Accellion data breach after confirming that data from the file-sharing system was stolen.

"Transport for NSW has been impacted by a cyber attack on a file transfer system owned by international company Accellion," TfNSW said.

Cyber Security NSW is managing the government's response to the Accellion breach, which has also impacted NSW Health.

"At this stage, investigations are undergoing. It's a complex matter, involving forensic work with external specialist providers to government," he said last month.

Other organisations to be impacted include the Australian Securities and Investments Commission (ASIC), SBS and the Reserve Bank of NZ. (Feb 2021)

What can we learn from these cyber-attacks?

Upon reflection of these recent attacks and the state of cyber security for critical infrastructure in Australia, we may ask following questions:

1. Does the Board have a full understanding and comprehension of the severity and scale of a potential cyber-attack?
2. What assurances are evidenced that a resilient cyber posture is in place and maintained?
3. With a fiduciary duty to manage risk, what actions should be taken to strengthen and maintain a resilient cyber posture?

Please share your experience. Your thoughts on these questions are welcome and encouraged and look out for further blogs which will address these three questions.