
CISCO
Wesfarmers Chemicals, Energy & Fertilisers has malware in its sights
HyFlex

When you are in the business of chemical and fertiliser manufacturing, risk management is a core consideration.

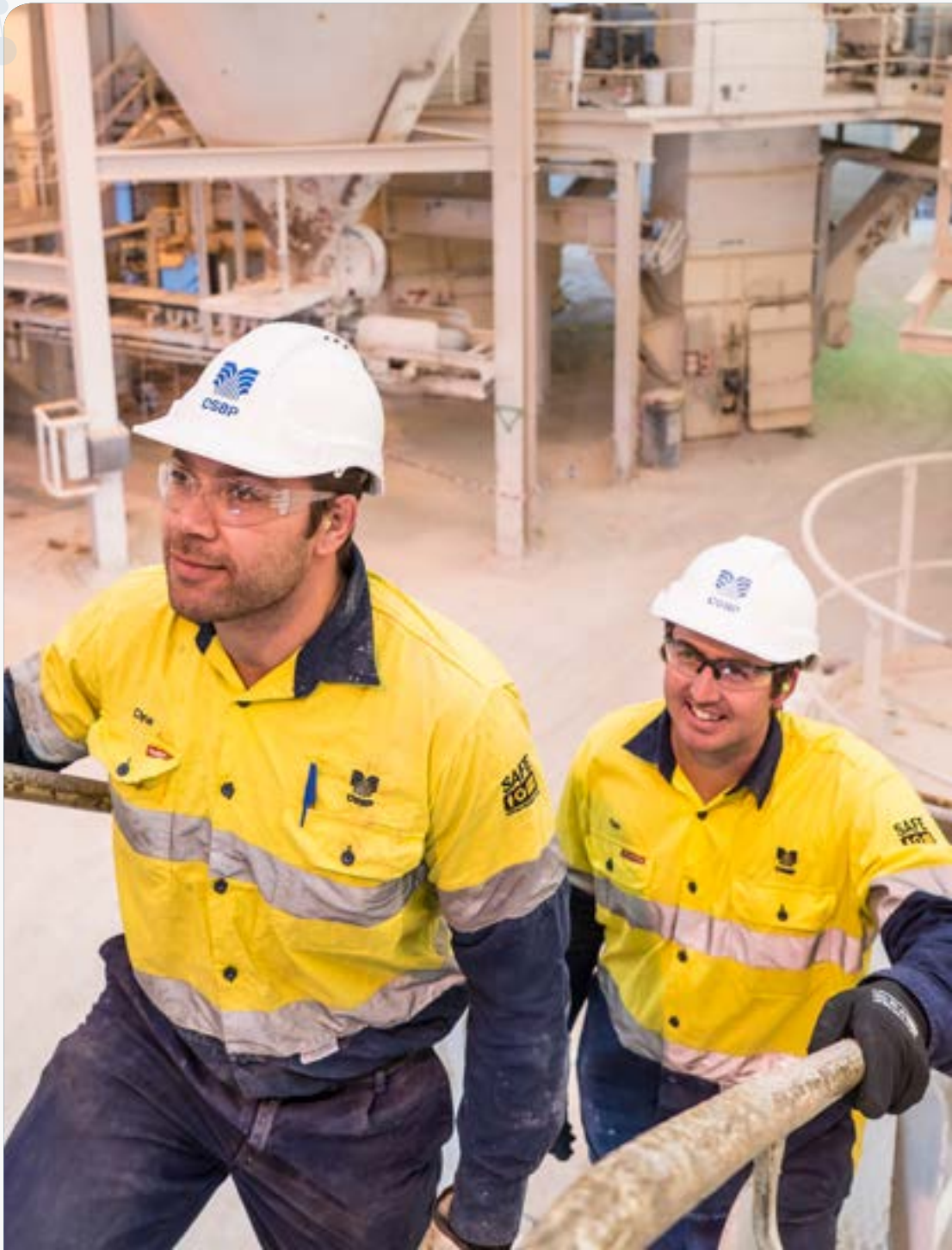
Wesfarmers Chemicals, Energy & Fertilisers (WesCEF), a subsidiary of Wesfarmers Ltd, is a thriving business providing essential chemicals and industrial products to key industry sectors around the world.

Following several years of strong growth, WesCEF has seen a sharp increase in the volumes of data and number of systems configured to connect more staff across more locations.

Recognising risk

At the same time, WesCEF has become more cognisant of the growing risk of cybersecurity attacks, and what they might mean in terms of reputational damage and real costs.

“Being threatened at any IT or OT [operational technology] level beyond our control could lead to reputational damage, loss of product, and health and safety issues ,” explains Alex Larson, CIO at WesCEF. “Converging our IT and OT was extremely important.”



Vulnerabilities

However, an audit of WesCEF's technologies and policies around cybersecurity revealed that due to the installation of different systems from different vendors over time, there was limited visibility and capacity to check performance against expectations.

But with the growing incidences of malware attacks like the recent WannaCry and Petya ransomware viruses, something had to change. Sweeping new data protection laws coming into effect in Australia in 2018, coupled with WesCEF's strict focus on safety, provided incentive for the organisation to proactively find a solution.

After taking stock of the problem WesCEF went to market in search of a solution, talking to several vendors in the security space. Following extensive consultations with senior Cisco engineers, it decided on a solution comprising the network specialists' entire security suite.

One of the most surprising things WesCEF realised as the deployment kicked off was that different security systems weren't talking to each other or generating proper reports.

The existing system was preventing proper oversight of what staff were doing online. Larson cautions that even legitimate websites ... have been found to harbour malware.

A number of malicious email atatchments for phishing and whaling were discovered. Whaling refers to specific phishing attacks targeting senior executives, and often contain a high degree of 'personalisation' including names, titles and other information intended to extract access to highly sensitive information. The existing system was

Wannacry

What: Malware
First appeared:
Friday 12 May 2017

Targeted: Computers running Microsoft Windows OS

How: Uses EternalBlue to exploit Server Message Block (SMB) vulnerability. Implants DoublePulsar backdoor, and uses that to install malware.

Infected, day one:
230,000+ computers in 150 countries
Including: UK's National Health Service, Spanish Telefonica, Fedex, Deutsche Bahn

preventing proper oversight of what staff were doing online.

Larson cautions that even legitimate websites providing news or other popular services have been found to harbour malware.

“One of the biggest security concerns for businesses is knowing what their staff are doing,” he says, adding that the deployment of Cisco’s security suite has not only increased protection for the organisation, but it has also led to changes in behaviour and company culture.

“[It] puts us in a stronger position to address threats and risky activity.”

Solutions

An important benefit for WesCEF was being able to check whether staff had the latest versions and patches for client software like Java and Adobe on their machines, and to deploy updates from one central location.

Deployment of the Cisco stack has also made it a lot easier for WesCEF to control and classify information according to its level of sensitivity, and to guard against ‘competitive’ data falling into the wrong hands.

This has put WesCEF in a better position to factor risk assessment into its R&D and innovation activities. While conceding it’s difficult to protect against every threat, Larson stresses that WesCEF now has a greater sense of confidence armed with effective tools to more quickly identify irregular activity on the network and assess what the impact has been.

“We now have the ability to proactively know ‘has it affected us?’.” If it has, Larson says, they are also empowered to find out where it came from and what the damage is. “It’s been an absolute godsend for us and puts us in a stronger position as far as business security goes.”

Using Cisco’s malware protection, Larson says WesCEF has not only bought insurance

to prevent malware from breaching the organisation's firewalls, but also effectively bloccked the path of viruses even if staff have already clicked on dubious attachments.

"As soon as a user clicks on an attachment it is immediately diverted to Cisco's security cloud to be verified before a user will be able to see its contents," Larson notes. He adds that WesCEF can now decrypt SSL, where previously it was limited to decrypting HTP.

A suite of cybersecurity solutions that fit seamlessly into WesCEF's existing environment are complemented by the expansion and security of its growing wi-fi network to support greater mobility and flexibility for the business.

Meanwhile, WesCEF has plans to establish on-site labs for building bespoke network and network security solutions, as well as increasing its engagement with various universities and innovation hubs, independently and via its ongoing partnership with Cisco.

We now have the ability to proactively know 'has it affected us?'. It's been an absolute godsend for us and puts us in a stronger position as far as business security goes.

Alex Larson
CIO
Wesfarmers Chemicals, Energy & Fertilisers

Find out more: watch Cybersecurity Insight sessions on-demand including Tech Talks, Threat Insights, and Customer and Business Insights.