How to maintain full treasury operations in the midst of a cyber-attack?

Follow Norsk Hydro's gold standard response

Adam Smith Awards
Best Cybersecurity Solution

About

Norsk Hydro is a fully integrated aluminium company with 35,000 employees in 40 countries on all continents, combining local expertise, worldwide reach and unmatched capabilities in R&D.[1]
Headquartered in Oslo, Hydro is on a mission to create a more viable society by developing natural resources into products and solutions in innovative and efficient ways. Hydro is present within all market segments for aluminium, with sales and trading activities throughout the value chain serving more than 30,000 customers.

The challenge

On 19 March 2019, Hydro was the victim of a cyber-attack targeting and impacting their technology infrastructure across their worldwide organisation. The incursion was a ransomware attack affecting 22,000 computers across 170 different sites in 40 countries with a message instructing: *"Your files have been encrypted with the strongest military algorithms…without our special decoder it is impossible to restore the data."*

With their normal computer systems unavailable, the entire workforce was forced to revert to using pen and paper. Production lines had to be switched to manual functions. To bolster existing employees, retired personnel were brought back to supplement the company's knowledge base, allowing for more hands-on operations.

Fortunately, Hydro had extensive disaster recovery plans in place, and while no one could have anticipated the extent to which operations could be impacted by a virus, their response as swift and strategic.

While the plants and operations teams were working day and night to find ways to keep machinery in production, Per Christian Lindgård, Head of Cash Management and his treasury team were doing the same for another critical piece of machinery – Hydro's Cash Management operation. Ensuring that critical payment functions, such as payroll, treasury and reporting, were not impacted by the attack was key to maintaining business-as-usual (BAU) operations for the company.

1 Source: https://www.hydro.com/en-US/about-hydro/key-facts/

J.P.Morgan

How to maintain full treasury operations in the midst of a cyber-attack?

Follow Norsk Hydro's gold standard response

The solution

The treasury team worked with its banking partners to institute cash management procedures that allowed the company to function during the **attack** without having to make the ransom payment.

In the immediate aftermath of the attack, **all accounts were closed**. The **treasury team worked closely** with its largest banking partner, **J.P. Morgan**, to ensure critical payments could be made in isolation from the attack, via a separate, **clean air-gapped network**. The team coordinated with the bank to closely monitor the company's cash movements to ensure that no fraudulent payments were made and to receive guidance and support from cyber experts within the bank.

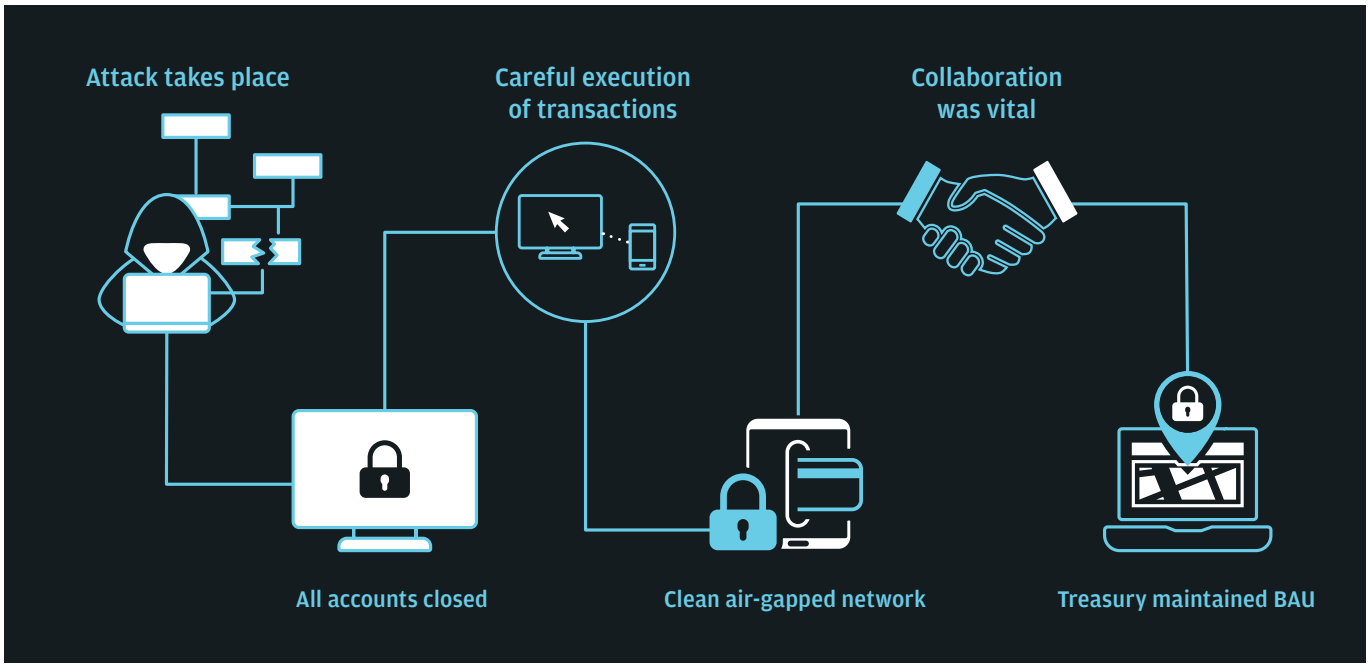
They also established a playbook with procedures to ensure settlement of margin calls and other larger value transactions to ensure terms were not breached. Then **smaller transactions were executed** via manual payments and completed on a country by country, division by division and case by case basis **until all treasury systems could be brought safely back online**.

Getting treasury fully back online was crucial for a company with two million commercial payments per year; **communication and close cooperation** with their internal teams and banking partners **was central** to achieving this.

As a result of this close collaboration, treasury was able to **maintain BAU throughout**.

The organisation also used this experience to test all of its systems and relationships – both internally and externally – and identified the need to implement host-to-host capabilities to help better prepare to execute mass payments in the face of future incidents.

This entire response, keeping treasury functioning under the most trying of circumstances, was accomplished by a small global cash management team of 10 professionals operating out of the company's Oslo headquarters.



J.P.Morgan

How to maintain full treasury operations in the midst of a cyber-attack?

Follow Norsk Hydro's gold standard response

The results

Hydro's effective cyber-incident response plans allowed the company to quickly respond and recover despite coming under attack from new ransomware known as "LockerGoga." Hydro's sustained resilience throughout the attack demonstrated the success of steps taken, which minimised the effects of the incursion.

According to BBC News, ***"Hydro's response to the incident is being described as 'the gold standard' by law enforcement organisations and the information security industry."***[2] Their approach was also recognised with the 2020 Adam Smith Award for Best Cybersecurity Solution.

Andrew Fullarton, Head of EMEA Natural Resources at J.P. Morgan is full of praise for the team at Hydro. "Rather than paying the ransom and attempting to conceal the attack, Hydro was honest and open, with the aim of helping others who might face a similar experience. They generously share their experience at treasury conferences so others can learn from their 'gold standard' response."

To learn more about how we can support your business, contact your J.P. Morgan representative.

[2] BBC news article: https://www.bbc.co.uk/news/business-48661152

J.P.Morgan