



A few challenging years in IR

Line Haugetraa

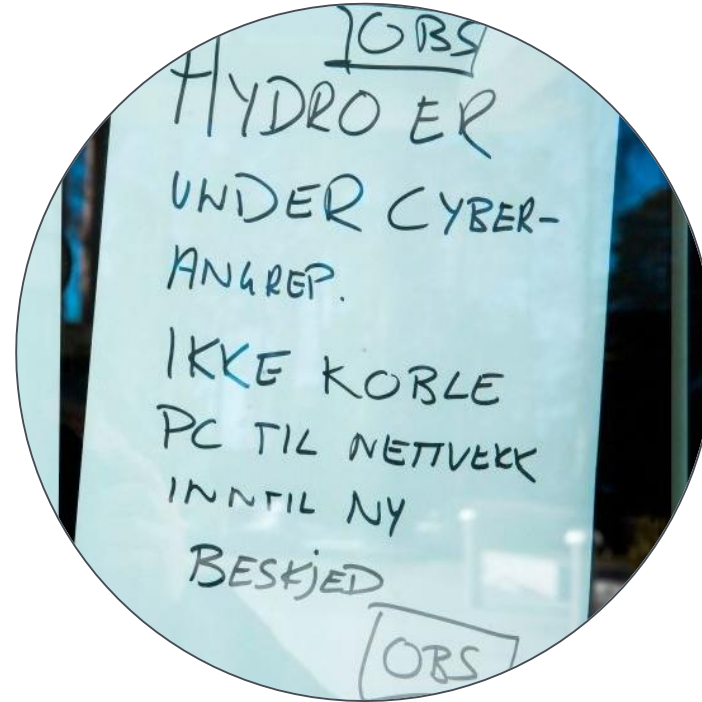
Head of IR Norsk Hydro ASA

It has been a few challenging years...

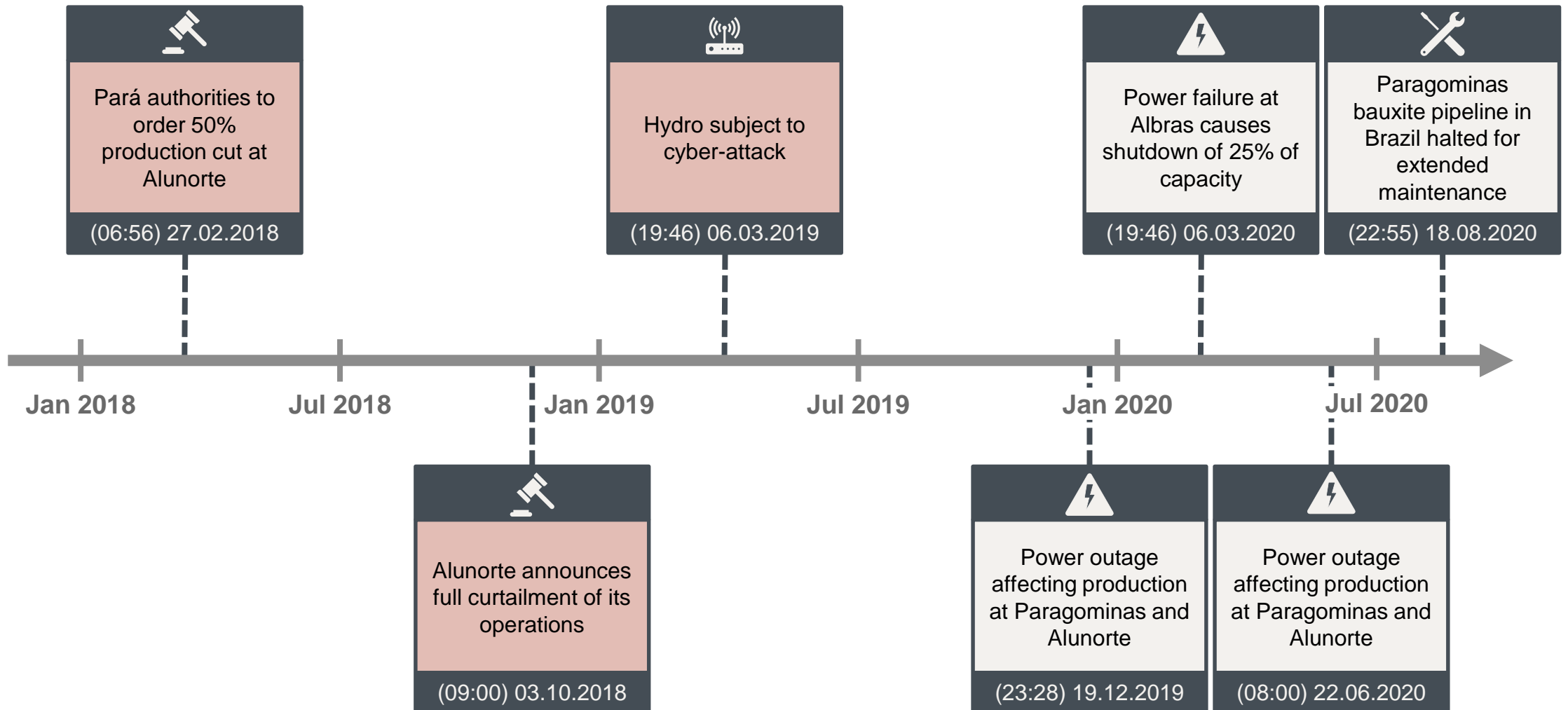
JAN 2018



MAR 2019



...«crisis management» took over the IR role...



When a crisis takes on a life of its own



What happens when the crisis takes on a life on its own...in a language you don't actually speak ...

- ... you find other stakeholders communicating (& controlling) “your” story...
- ...information is scarce and incomplete ... it's complex situation... what is important, what is not, what is actually happening, what is true? What is false?
- ...Brazilian politicians start posting on facebook

At the same time you are

- ...far away, with a limited information flow
- ...your work hours now include Norwegian and Brazil time... (and most of the hours in between)
- ...you are constantly on the phone with the markets....with no actual news

How do you take control? How do you ensure compliance? How do you do your job?

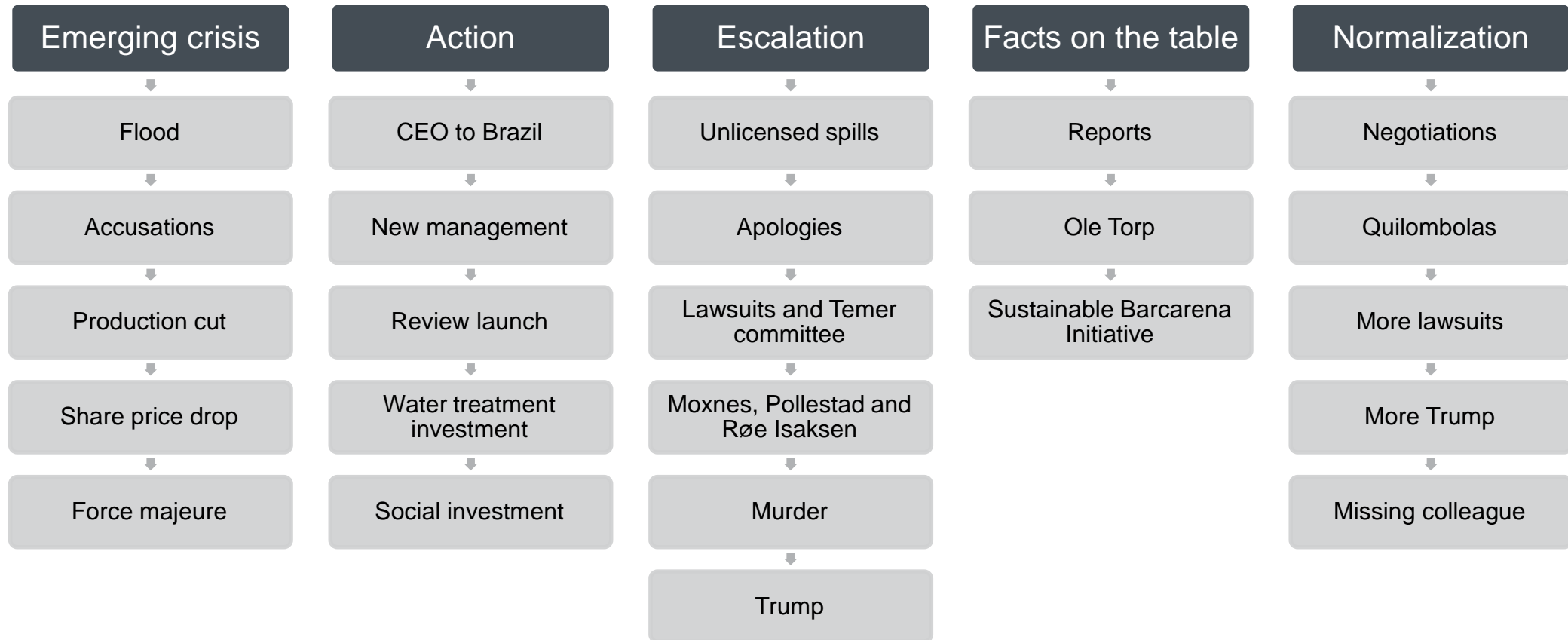


Different approaches required for different stakeholder

Internal	<ul style="list-style-type: none">• Engage employees through timely and frequent information• Leadership communication and digital channels
Financial markets	<ul style="list-style-type: none">• Timely updates, in compliance with OSE regulations• Meetings with key shareholders
Political & authorities	<ul style="list-style-type: none">• Correcting the understanding of the situation through proactive dialogue• Meetings and major outreach to key political stakeholders
Experts and NGOs	<ul style="list-style-type: none">• Presenting the facts of what has (and has not) happened• NGO cooperation in Barcarena, major outreach in Norway and Brazil
Communities	<ul style="list-style-type: none">• Acknowledging that Hydro has not lived up to expectations• Seek partnership and agree on way forward
Customers	<ul style="list-style-type: none">• Coordinated customer communication across the value chain• One voice, different accents
Media	<ul style="list-style-type: none">• Fact based communication• Background dialogue with important journalists/editors in Brasilia/Sao Paulo

Crisis that kept escalating

Jan - Jun 2018



Getting back control...clear and timely communication is key

Communication objectives and principles

Objectives:

- Protect reputation
- Instill trust, enable and empower employees
- Timely market information

Principles:

- Transparency and frequency
- Humble and fact-based tone of voice
- One step ahead
- Show don't tell – demonstrate

Main channels

- Messages from corporate (internally): Line communication, email, intranet, NewsApp
- Messages from corporate (externally): The new hydro.com, Facebook, OSE
- BAs: Relevant channels for line communication

Main channels

- 09:00 CET: Daily internal update
 - 08:00 End –user (technical comms.)
 - 09:00 Townhall / internal briefing / webcast
- 09:00 CET: Daily external update
 - 08:00 Press release / OSE release
 - 14:00 Analyst + press briefings (conference call or webcast open for employees)

Finally Brazil stabilized...then the Cyber-attack hits

BUSINESS

Norsk Hydro Is Hit by Ransomware Cyberattack

The company, one of the world's largest aluminum producers, says its operations were crippled

By [Alistair MacDonald](#) and [Dominic Chopping](#)
Updated March 19, 2019 1:46 pm ET

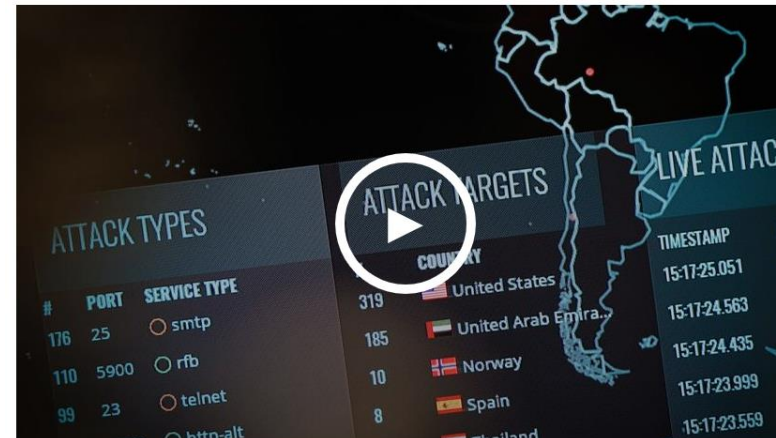
Cybersecurity

Big Norwegian Aluminum Producer Suffers Extensive Cyber Attack

By [Jonas Cho Walsgard](#), [Elena Mazneva](#), and [Mark Burton](#)

March 19, 2019, 8:41 AM GMT+1 Updated on March 19, 2019, 5:07 PM GMT+1

- ▶ Company says attack originated in U.S.; some plants halted
- ▶ Sustained disruption could cut supply of specialized products



Cyber Attack Cripples Aluminum Producer Norsk Hydro

Basic resources

Hacker virus holds Norsk Hydro to ransom

RICHARD MILNE — OSLO
HENRY SANDERSON AND
MARTIN COULTER — LONDON

Norsk Hydro became the latest company to be hit by hackers in a ransomware attack as one of Europe's leading aluminium producers suffered stoppages at several of its plants.

The Norwegian company said it had switched many of its smelters to manual operation as it isolated all its global factories and stopped production at some plants that make aluminium components after the attack that started late on Monday in the US.

"The situation for Hydro through this is quite severe. The entire worldwide network is down," said Eivind Kallevik, finance director.

Hydro is rushing to identify the encryption virus behind the attack and hopes to use back-up data to restore its IT systems rather than pay the ransom. Norwegian cyber authorities said they had yet to identify the virus or the hackers but one hypothesis was that it was ransomware called LockerGoga, thought to be used this year against French company Altran Technologies.

A long line of companies from AP Moller-Maersk to Saudi Aramco have been targeted by hackers in recent years, lifting cyber security up the boardroom agenda. In January Nyrstar, Europe's largest zinc producer, said it was hit by a cyber attack that shut down some of its IT systems.

Hydro officials said that they were unable to use their computers but were

"The situation for Hydro . . . is quite severe. The entire worldwide network is down"

able to communicate via mobile phones and tablets. Mr Kallevik said Hydro was not yet able to quantify the financial impact but confirmed it had cyber insurance. Shares in Hydro fell as much as 3.4 per cent but recovered to trade down 0.6 per cent yesterday afternoon.

Hydro is one of the biggest suppliers of aluminium as well as alumina, a raw material used to make the metal.

Smelters — used to extract aluminium — are costly to shut down so Hydro

switched its Norwegian plants to a "higher degree of manual operations". Its hydroelectric power plants in Norway, bauxite and alumina operations, and smelters outside Norway were all running as normal, the company added.

Its downstream operations, making rolled products and other components from aluminium, were more affected with some "temporary stoppages".

Mr Kallevik said the plants had customer order data for yesterday but refused to speculate when they would run out of that. He added that the priority was now to identify the virus and attempt to find the cure. "The longer the virus is active, the more it will have an impact," he added.

Andrea Carcano, co-founder of cyber security firm Nozomi Networks, said industrial groups were making themselves vulnerable by bringing in internet-enabled technology into factories.

"As industrial organisations automate and digitise plant floors, the security of these new processes must be forethought to reduce the risks of potential attacks," she said.

rippled

renewable-energy
ther internally,

But now we are ready...

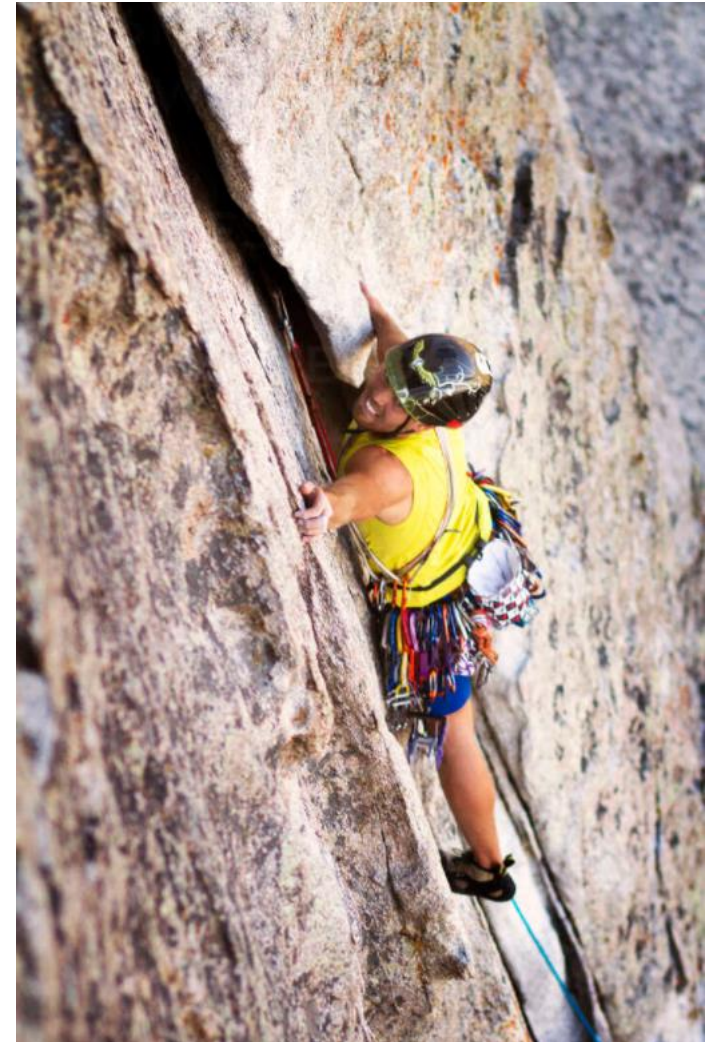
What does this do to the IR function of a company?

Focus on “surviving the day” – short term over long term focus

Investors and analysts start losing confidence in your company

There is frustration

You are no longer discussing your equity story with investors...wait ..what is actually our equity story...?





Hydro

We are aluminium



08:31 - 19th March 2019

Hydro subject to cyber attack

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday (CET), impacting operations in several of the company's business areas.

IT-systems in most business areas are impacted and Hydro is switching to manual operations as far as possible. Hydro is working to contain and neutralize the attack, but does not yet know the full extent of the situation.

Published: March 19, 2019



14:41 – 19th March 2019

Update: Hydro subject to cyber attack

As communicated earlier today, March 19, Hydro has been subject to an extensive cyber-attack, impacting operations in several of the company's business areas.

Hydro has isolated all plants and operations and is switching to manual operations and procedures as far as possible.

Hydro's main priority is to continue to ensure safe operations and limit operational and financial impact. The problem has not led to any safety-related incidents.

Relevant authorities have been notified and are supporting Hydro in the efforts to resolve the problem.

Operational status

Energy: Production running as normal

Bauxite & Alumina: Production running as normal

Primary Metal:

- Primary plants in Norway running as normal, with higher degree of manual operations
- No indication of impact on primary plants outside Norway
- Remelters running as normal, with high degree of manual operation

Extruded Solutions and Rolled Products:

- Lack of ability to connect to the production systems causing production challenges and temporary stoppage at several plants

Hydro is working to contain and neutralize the attack but does not yet know the full extent of the situation.

It is too early to indicate the operational and financial impact, as well as timing to resolve the situation. Hydro is doing its utmost to limit the impact on customers.

For further update, Hydro will host an analyst/press conference at its corporate headquarters at Drammensveien 280, Oslo, at 15:00 CET today and can also be seen on web TV.

Related links

[Analyst/press conference webcast](#)

Contacts



Stian Hasle
Investor Relations

+47 97 73 60 22
stian.hasle@hydro.com



Halvor Molland
Senior vice president,
Media Relations

+47 92979797
halvor.molland@hydro.com

08:39 – 19th March 2019

Update on the cyber attack on Hydro

Hydro has made progress in securing safe and stable operations across the company, following an extensive cyber attack that hit on Tuesday.

Hydro's technical team, with external support, has succeeded in detecting the root cause of the problems and is currently working to validate the plan and process to restart the company's IT systems in a safe and sound manner. However, it is still not clear how long it might take restore stable IT operations.

As communicated on Tuesday, Hydro was subject to an extensive cyber attack, impacting operations in several of the company's business areas.

Following detection of the problem, Hydro isolated all plants and operations and switched to manual operations and procedures. The main priority continues to be to ensure safe operations and limit operational and financial impact.

"I'm pleased to see that we are making progress, and I'm impressed to see how colleagues worldwide are working around the clock with dedication to resolve this demanding situation and ensure safe and sound operations," says Hydro's CFO Eivind Kallevik.

"I would also like to complement our external technical partners who have done an important job in supporting our efforts, and also relevant authorities, who handle the issue with the diligence it deserves," Kallevik says.

Most operations are running, ensuring deliveries to customers according to specifications, with some more manual operations than normal.

Update on operational status

Energy: Production running as normal

Bauxite & Alumina: Production running as normal

Primary Metal: Production running as normal, with higher degree of manual operation

Extruded Solutions: Lack of ability to connect to the production systems have caused production challenges and temporary stoppage at several plants. Progress has been made, with the expectation to restart certain systems during Wednesday which would allow for continued deliveries to