HERBERT SMITH FREEHILLS

MINERS LEAD ON OCCUPATIONAL HEALTH AND SAFETY. BUT WHAT ABOUT DIGITAL HEALTH AND SAFETY?

09 April 2021 | Australia
Legal Briefings

With cyber attacks all over the news – and cyber security firm, Secolve, warning that miners and contractors could be increasingly in the cross-hairs – we look at where your operations could most be at risk, and what you can do to reduce the risk of being the next victim.

In 2019, *International Mining* reported that Swiss mining and metals processer Nystar was hit by a cyber attack which necessitated key IT systems, including email, being shut down at both corporate and operational sites. It would be easy to dismiss such an event as an isolated situation (especially as mining operations were not directly impacted) – however, the same publication had earlier reported that **54% of mining companies had experienced a significant cyber incident in the previous 12 months**.

Increasing international interconnectivity has resulted not only in significant knowledge, productivity and efficiency gains but, on the flip side, also an expanding and evolving cyber threat environment which is increasingly capable of posing existential threats. The Australian media has recently reported on the impact of high profile cyber events (think Nine Network and Toll), and for all Australian organisations, accepting and adapting to this changing environment, where state, quasi-state and criminal actors operate with seeming impunity, is critical. The 'new normal' is not limited to COVID considerations. The need to adapt is even more so in the mining sector, where the threat vectors are likely to be broader than those confronting many other enterprises operating in Australia.

WHERE YOUR OPERATIONS COULD BE AT RISK

Much of the recent media reporting has focused on the rise in two types of cyber attacks:

- **ransomware attacks**, where large volumes of data are encrypted (and increasingly also exfiltrated) and a ransom being demanded for the decrypt key to regain access to data, with the added threat that if a ransom is not paid, sensitive data that has been exfiltrated will be made available; and
- **distributed denial of service** (or **DDoS**) attacks, such as that which recently impacted the NZX, and where a targeted service or network is overwhelmed with a flood of internet traffic.

Such attacks focus on compromising sensitive data, and while the mining sector does not hold the volume of personal information as a supermarket chain, for example, highly sensitive mining data (like pricing data, inventory/scheduling information, and employee data including salaries and benefits) remains a high value target for not only organised criminal enterprises, but also nation states.

However, mining companies utilise operational technology (OT) in an increasingly sophisticated way in the extraction and operations processes. A well-planned cyber attack focusing on a mining company's autonomous vehicle fleet or IoT systems, for example, could severely disrupt business and adversely impact production. In a worst case scenario, health and safety can be compromised: in 2017, malware which is commonly referred to as "Triton", and which targets industrial control systems, was deployed against a Saudi Arabian petrochemical plant with the intention of interfering with emergency safety controls. Such cyber sabotage or cyber espionage are threats which are more pronounced in the mining sector.

HOW YOU CAN STAY AHEAD OF THE GAME

Effective technology tools and processes can greatly enhance cyber resilience – for example, maintaining version control on applications and deploying emergency patches/updates without delay, and implementing security tools and processes such as virus detection systems and penetration testing.

However, a key plank (perhaps *the* key plank) in any organisation's cyber resilience strategy is the **culture of the workforce**. In assessing cyber-readiness, there must be a clear focus on the internal information environment, including:

- staff on-boarding processes;

- initial and ongoing education and training; and
- staff at all levels embracing the importance of data.

Each employee has a critical role to play in managing cyber risk – email phishing remains an effective means of launching malware, and disclosure of sensitive information is still often caused by 'fat finger' errors. In this respect, mining companies, which have an historically strong and market-leading focus on occupational health and safety, can leverage from this physical safety culture to drive improvements in digital safety culture. Accepting the critical importance of a safe and resilient work environment is already a given.

HOW WE CAN HELP – SEVEN AREAS TO CONSIDER

Our multi-practice cyber team helps clients on all manner of digital health and safety matters – from proactively reducing the threat of successful cyber attacks through to advising and assisting on breach response. We would be happy to discuss with you how we can:

- undertake an information risk 'health check' across your integrated organisation;
- advise the board on its obligations with respect to cyber resilience;
- provide targeted training to different teams and disciplines;
- conduct cyber attack simulation exercises;
- advise on cyber attack response requirements, including advising on notification requirements or expectations with respect to regulators, law enforcement, other government agencies, continuous disclosure obligations and insurance;
- assist with ransom payment demands; and
- advise in connection with post-attack remediation requirements.

Read more on our **Mining Notes Blog**.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

PETER JONES
PARTNER, SYDNEY

+61 2 9225 5588
peter.jones@hsf.com

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

LEGAL NOTICE