MINING

Precious ore, precious data

A digital future opens an old industry to new threats, says Brunswick's CAROLE CABLE

No one knows exactly what the mine of the future will look like, but we can be sure of one thing: it will be a target for hackers. Mining may not seem an obvious place to find cybersecurity risks, but the industry is transforming fast. Commodity prices have fallen 52 percent since 2011 and mining productivity is down 3.5 percent per year over the last 10 years, according to a 2015 McKinsey report. In response, the industry has turned to digital and technological innovation to help preserve cash in the short term, and capture value over the long term.

Mining operations are often in remote locations, with variations in geology, metallurgy and weather extremes. New technology is helping mitigate such variability by lowering risk and cost while increasing safety and productivity. "We believe this to be the future of mining," says Pedro Fuenzalida, Innovation Manager at Antofagasta Minerals. Analytics can "deliver a step change in productivity," he says.

Digital tools already move equipment fleets and driverless trains, schedule maintenance and manage the global supply chain. Drones and scanning equipment create 3-D maps of underground areas, and robots are being developed to mine hard-to-reach resources. Rio Tinto's fleet of autonomous trucks has driven the equivalent of 98 times around the earth to deliver loads 24 hours a day.

"Our operations are increasingly digitized," says Richard Williams, COO of Barrick Gold Corporation. But this progress has a downside. "Data flows from one point to another, which makes it open to attack," he says.

In 2012, Saudi Aramco revealed a cyber assault on its systems, to "stop the flow of oil and gas to local and international markets," Abdallah al-Saadan, Aramco's Senior Vice-President of Finance, Strategy and Development, said at the time. While it didn't succeed, damage was still done.

In 2015, Canadian company Detour Gold was hacked, putting at risk credit card numbers and employees' personal data. And in 2016, Canada's Goldcorp had 14.8 gigabytes of sensitive data accessed and posted on a public website by "hacktivists," with a message railing against "corporate racism, sexism and greed."

Meanwhile, the industry has been poor at disclosure and communication of how it assesses, manages and mitigates cyber risk. Of the top 20 global mining companies, just 12 mention cybersecurity as a risk in their 2015 annual reports. Among them, disclosure varies widely: from a minimal statement saying the topic was discussed by the Audit and Risk Committee, to a vague outline of the potential impact of attacks. Only one classified a potential breach as a "reputational risk."

As the mining industry depends more on digital technology, stakeholders will look for a balance between transparency and secrecy, creating value and protecting it. This is not an IT issue. Everyone in the company must take responsibility. "People see risk as a separate subject managed by specialists," Williams says. "But cyber risk being managed by IT is the same as leadership being managed by HR – it feels like a function and is not owned at the highest level of the organization."

CAROLE CABLE is a Partner in Brunswick's London office and co-leads the Global Energy and Resources practice.

NO BUSINESS IS IMMUNE

Anyone with data can be a target, says Brunswick's Will Rasmussen

Consider this scenario: a hack into the interconnected systems controlling major office buildings causes chaos by triggering fire sprinklers, creating sauna-like temperatures and manipulating critical equipment. "It's not something that real estate investors really had to think about before, but it's definitely on our radar screens now," says Tom Murray, a Principal Partner at New Mill Capital, a real estate investment firm.

No business that stores or transmits information is immune from cyber attack. Some sectors have so far avoided data breach headlines, but threats and risks continue to increase.

Antony P. Kim, Global Co-Chair of the Cybersecurity and Data Privacy team at the law firm Orrick, says the number of businesses boosting preparations has increased sharply. "No organization is too boring or unattractive to a hacker," Kim says.

Sectors with little history of attacks are often at greater risk. Recent reported hacks in the computer systems of cars, and even a jet's in-flight entertainment system, shook the transportation sector. In 2016, hackers manipulated a US water treatment plant. A year earlier, a German steel mill reported massive damage after an attack disabled blast furnace controls. Surprising targets include small businesses and nonprofits.

"Ask these questions," Kim says. "Do we use computers? Do we use the internet? Do we create or handle data? If your answer to these questions is yes, then you are a viable target for the bad guys."