A Catastrophic Catalyst

"There are two types of mining companies: the ones that can foresee risk and act, and those that need to be pushed."

Deepwater Horizon. Samarco. Grenfell Tower. Fukushima.

Four well-known contemporary catastrophic events that have shaped their respective industries. Traditionally, the resources sector has required the occurrence of a significant catastrophic event before long overdue corporate and regulatory action is taken. This trend is expected to extend to cybersecurity in the mining industry, with 98% of survey respondents identifying that such an event would be required to drive a sector-wide response.

The threat to industrial systems should not be underestimated. We have already seen the rapid deployment of new and more destructive cyber-attacks across the industrial sector:

- Nuclear centrifuges in Iran damaged by malicious commands sent by Stuxnet destructive malware in 2010;
- Blast furnace in German steel mill damaged by malware which destroyed control system in 2014; and
- Interruptions to the Kiev power grid by the BlackEnergy malware attack in 2015.

A cybersecurity incident in the mining industry could take a variety of forms. A majority of respondents have identified that a physical incident would be more likely to galvanise a sector-wide response than a data breach. First movers in protecting industrial operating systems and suppliers who engage with this challenge will realise significant safety benefits.

FIGURE 22

WE ASKED: WHAT LEVERS DO YOU BELIEVE WILL DRIVE A SECTOR-WIDE RESPONSE TO CYBERSECURITY IN THE MINING INDUSTRY?

By % of respondents given two options

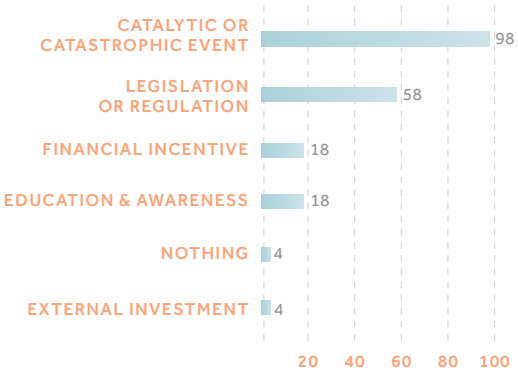

FIGURE 23

WE ASKED: WHAT CATALYTIC EVENT, CAUSED BY A CYBER-ATTACK, IS MOST LIKELY TO GALVANISE SECTOR-WIDE RESPONSE TO CYBERSECURITY?

By % of respondents given three options