10. CYBER SECURITY

RISK DESCRIPTION

We recognise the importance of the confidentiality, continuity, integrity and security of our data and production systems.

As a mining company, we may be under threat of cyber attacks from a broad set of attacker groups, from 'hacktivists' and hostile regimes to organised criminals.

Their goals include a desire to take advantage of the role that mining plays in regional and global supply chains as well as in national economies. Certain groups may also attempt to exploit vulnerabilities created by the industry's heavy reliance on automated operational systems. In our case, this could include initiatives such as Operations Technology and Information Technology (OTIT) Integration and Digital Mine (see pages 50 to 65).

RESPONSE/MITIGATION

During 2018 we developed a set of initiatives under our 'Cyber Security Programme & Threat Assessment' project, supported by external advisors. The objective of the programme is to identify the cyber security risks to which our Company is exposed to and align them to our mission and business strategy.

In line with best practice, our approach is based on two key frameworks:

- The US National Institute of Standards and Technology Cyber Security Framework (NIST CSF) which outlines how companies can assess and improve their ability to prevent, detect and respond to cyber attacks.
- Control Objectives for Information and Related Technologies (COBIT), which was created by ISACA, the international professional association for IT management and governance, to provide an implementable set of IT-related controls, processes and enablers.

Our approach will also be based on the MITRE ATT&CK™ which is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber security product and service community. A governance model, continuous risk assessment and Information Security policies will form the basis for our OTIT operational assurance which will support the digital transformation of Fresnillo in the coming years.

DESCRIPTION OF RISK LEVEL

As cyber security is an increasing threat to the industry, the Audit Committee continues to monitor and oversee this risk.

Our plan for 2019 is to focus our efforts on risk mitigation projects designed to protect information and key assets, according to the risk appetite set by management.

KEY RISK INDICATORS

- Total number of cyber security incidents affecting our Company.
- Number of media mentions related to cyber security issues affecting the mining industry.

RISK APPETITE

LOW

Risk rating (relative position)

2018: Medium (10)

2017: Medium (10)

LINK TO STRATEGY

2 3

CHANGE IN HEAT MAP

=