8 – Cyber security

RISK DESCRIPTION

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

As a mining company, we can be under threat of cyber attacks from a broad set of groups of attackers, from 'hacktivists' and hostile regimes, to organised criminals. Their objectives include a desire to take advantage of mining's role in regional and global supply chains, as well as in national economies.

Some groups may also attempt to exploit vulnerabilities created by the industry's heavy reliance on automated operating systems.

The following are the top eight cyber security and privacy risks that have been identified through workshops with business units, operations and IT. These risks comprise Peñoles/Fresnillo overall cyber security and privacy risk profile:

1. Corruption of data – Critical data where any modification can have adverse impacts.
2. Unauthorised access – Cyber security and privacy incidents due to unauthorised people or incorrect access permissions.
3. Breach and data theft – Disclosure of critical and sensitive Company data by an internal or external source.
4. Business disruption – Disrupting key applications or systems for a period of time.
5. Lack of cyber security ownership – Failure to take responsibility for implementing and adopting cyber security practices on a daily basis.
6. Non-compliance – Cyber security and privacy incidents resulting in non-compliance with applicable regulations, including privacy.
7. Health and safety incidents – Breach of availability, integrity or confidentiality of data which impacts health and safety.
8. Halt or loss of operations – Cyber security and privacy incidents which result in loss of operating licence or cause delay to operations.

FACTORS CONTRIBUTING TO RISK

- Cyber risks have increased significantly in recent years owing in part to the Covid-19 pandemic and the proliferation of new digital technologies, the increasing degree of connectivity and a material increase in monetisation of cybercrime.
- Theft of information through social engineering and 'phishing' campaigns (fraudulent attempts to obtain sensitive information or data, such as usernames or passwords, by appearing to be a trustworthy entity in an electronic communication).
- Using non-secure means of communication with the Company's networks can lead to viruses, data leakage, information theft, malware and ransomware.

CONTROLS, MITIGATING ACTIONS AND OUTLOOK

Our information security management model is designed with defensive structural controls to prevent and mitigate the effects of computer risks. It employs a set of rules and procedures, including a Disaster Recovery Plan, to restore critical IT functions in the event of an attack.

Our systems are regularly audited to identify any potential threats to the operations and additional systems have been put in place to protect our assets and data.

We have implemented a training and awareness programme, which is designed to increase awareness of cyber risk and ensure that employees take the appropriate actions.

We have invested in global IT security platforms in order to proactively monitor and manage our cyber risks. We conduct routine third-party penetration test to independently confirm the security of our IT systems and we seek to enhance the monitoring of our operational technology platforms.

During 2020, we introduced a set of new initiatives to improve our cyber security programme, supported by external advisors. The main objective of the programme is to identify and manage cyber security risks and align them with our business mission and strategy.

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

- The US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) that describes how companies can assess and improve their ability to prevent, detect and respond to cyber attacks.
- Information Control Objectives and Technologies to Others (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 facilitators.

Our approach is also based on the MITRE ATT&CK™ which is used as the basis for the development of specific threat models and methodologies in the private sector, government and in the cyber security products and services community.

A governance model, continuous risk assessment, information security policies, awareness-raising campaigns and training will form the basis of our IT/OT operational guarantee.

Our plan for 2021 is to focus our efforts on risk mitigation projects designed to protect key information and assets, in accordance with the risk appetite established by management.

COVID-19 PANDEMIC IMPACT

With the Covid-19 pandemic, this risk has increased mainly due to 'phishing' attacks and the increase in home working.

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.

LINK TO STRATEGY

2 3

RISK APPETITE

Low

CHANGE IN HEAT MAP

Increasing

RISK RATING (RELATIVE POSITION)

2020: Medium (8)

2019: Medium (10)