CASE STUDY: Managing cybersecurity risks

We recognize that cyberattacks represent a potentially significant risk to our company and industry.

With oversight from Cheniere's Vice President and Chief Security Risk Officer (VP-CSRO), our Chief Information Security Officer (CISO) manages the technology security team. This team is responsible for maintaining our technology defense posture and program, educating and informing Cheniere's users about information security risks and how best to avoid them, and also for developing end-to-end incident response and recovery plans throughout the company. Our VP-CSRO and CISO report cybersecurity issues and performance to the board on a quarterly basis.

Cheniere's Information Technology Security Policy follows an "identify, assess and mitigate" approach to cybersecurity, in alignment with the National Institute of Standards and Technology's Cybersecurity Framework. We conduct regular internal audits and risk strategy sessions to assess cybersecurity threats and respond accordingly. To complement this effort, we contract with third parties to perform facility and system penetration tests, compromise assessments and security maturity assessments of both our corporate and operational networks. Cheniere also maintains a comprehensive cybersecurity and training program to proactively help our personnel identify and assist in mitigating cyber and data security threats.