Cybersecurity

We are committed to providing robust cybersecurity services to protect the reliability and availability of information and technology infrastructure and services.

Companies in the energy industry own and manage major pieces of critical infrastructure that are vital not only to company operations but also to the nation's economic and well-being. Upstream, midstream, and downstream operations are valuable targets for cyber threats from adversaries with a variety of motives—from personal profit to industrial espionage to economic disruption.

Identifying and Mitigating Cybersecurity Risks

At Gibson, we believe in the continued enhancement of controls to protect the confidentiality, integrity, and availability of corporate and operational systems, networks, and data assets. We regularly assess cybersecurity maturity and capabilities both through internal audits as well as independent third-party engagements; including an annual maturity assessment against the National Institute of Standards and Technology (NIST) cybersecurity framework; and regular performance of internal and external Penetration testing. Annually we fund programs and projects to continually improve our cybersecurity capabilities and strengthen our maturity level. For additional discussion on Technology risks Gibson has identified related to information security, please refer to our Annual Information Form.

Training and Compliance

We are committed to ensuring employee and contractor awareness and understanding of cybersecurity responsibilities. All personnel are required to complete an Annual Cybersecurity Training, which is designed to introduce/update employees on the most common threats that we face from a cybersecurity perspective. On a quarterly basis, additional courses are provided to ensure personnel are familiar with ways to stay cyber safe based on the latest cyber threat environment.

We also measure effectiveness of our cybersecurity processes by implementing regular phishing simulations. Through this, we hope to enable employees to better recognise potential phishing attempts while also identifying opportunities to strengthen our information security controls.

Cybersecurity Governance

Our SVP & Chief Administrative Officer has executive oversight of our cybersecurity strategy and performance.

All employees and contractors must acknowledge and adhere to our IT Assets Acceptable Use Policy, which defines the expectations of all who utilize Gibson's IT assets to protect the organization from the impact of cyber risk.

CYBER ATTACKS RECOGNIZED BY THE WORLD ECONOMIC FORUM AS ONE OF THE TOP 10 GLOBAL LONG-TERM RISKS