CYBERSECURITY

As a trusted operator and critical provider of infrastructure in the Canadian energy space, we are committed to ensuring that robust cybersecurity services are in place to protect our data and the reliability of our services.

We recognize the importance of the infrastructure we manage and how vital it is not only to our operations, but to the nation's economy and well-being. Upstream, midstream and downstream operations are all targets for cyber threats from adversaries with a variety of motives such as personal profit, organized crime, industrial espionage and economic disruption.

Identifying and Mitigating Cybersecurity Risks

We conduct regular assessments of our capabilities and cybersecurity maturity, through both internal audits and independent third-party engagements. We assess ourselves against industry-leading standards such as the Centre for Internet Security (CIS) Critical Security Controls, National Institute of Standards and Technology (NIST) cybersecurity framework, internal vulnerability assessments and regular internal and external penetration testing. We continue to fund programs and projects to improve our cybersecurity capabilities and further increase the maturity level of our program.

We have a Cyber Incident Response Plan (IRP) that enables our organization to effectively identify, protect and recover from cybersecurity threats and will continue to focus on further improving and embedding our practices. For additional discussion on Technology risks Gibson has identified related to information security, please refer to our Annual Information Form.

Training and Compliance

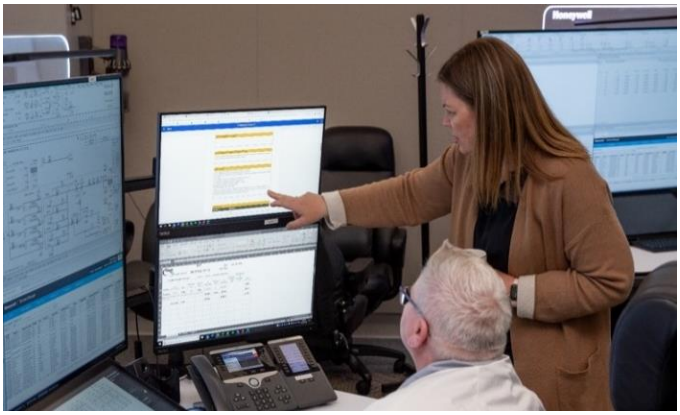
We believe our employees are one of the best forms of defense against cyberattacks, and we are committed to enhancing their awareness and understanding of cybersecurity responsibilities. All personnel must regularly complete Gibson's cybersecurity training, which is designed to increase awareness of new and emerging cybersecurity threats. Specific remote work training is also provided to ensure personnel understand ways to stay cyber-safe while working from home or away from the office.

We assess the effectiveness of our cybersecurity training through regular threat simulations and the monitoring of compliance with mandatory training requirements. As of 2023, 100% of employees completed cybersecurity awareness training.

Cybersecurity Governance

Our Senior Vice President & Chief Administrative and Sustainability Officer has executive oversight of our cybersecurity strategy and performance, while the Audit Committee maintains Board oversight. Cybersecurity updates are provided to the Board on a quarterly basis.

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



CYBER ATTACKS RECOGNIZED BY THE WORLD ECONOMIC FORUM AS ONE OF THE

TOP 10 GLOBAL LONG-TERM RISKS