Cybersecurity

Why it's important

As a provider of essential energy infrastructure, we adopt the same attitude toward cyber safety as we do toward our physical safety: staying alert, cautious and ready to respond immediately to any concerns and threats. Cybersecurity is a vital aspect of how we help protect our Company and customers.

Governance

The following list outlines how we maintain oversight of cybersecurity from the Board level to individual employees.

- **Board of Directors:** The Audit, Finance and Risk Committee of our Board of Directors has the highest level of oversight of cybersecurity matters, including the integrity of financial data, the security of the cyber landscape, and operational risk and controls, and receives a quarterly report on these topics to review.
- **Chief Information Security Officer:** Enbridge has a dedicated Chief Information Security Officer and team responsible for driving a culture of safe and secure cyber behaviors across the Company. Our Chief Information Security Officer has oversight on matters related to information security.
- **Employees:** Every employee has the responsibility to help us safeguard our data and digital assets.

Policies

Our overarching Cybersecurity Policy and supporting standards, processes and guidelines govern the protection of the Company's technology assets to manage cybersecurity risks, threats and vulnerabilities. This policy, along with the Privacy Policy, emphasizes and strengthens the protection of personal information to prevent unauthorized access, loss or theft of data. This year, we introduced our Artificial Intelligence (AI) Policy that sets clear guidelines on how AI can be used safely and responsibly by our employees.

Our cybersecurity practices align with the National Institute of Standards and Technology (NIST) framework. We engage a third party to conduct an annual assessment of our practices benchmarked against our oil and gas industry peers and have been ranked in the top quartile using NIST's six pillars (govern, identify, protect, detect, respond and recover) of a successful cybersecurity program. We also align our cybersecurity program with applicable requirements and industry best practices such as International Organization for Standardization (ISO) 27001; Transportation Security Administration (TSA) Pipeline Security Directives and Guidelines; American Petroleum Institute (API); Canadian Standards Association (CSA); and U.S. Securities and Exchange Commission (SEC).

Goals and metrics

- Ensure employee awareness and understanding of security responsibilities: 100% completion of annual certification and training.
- Achieve internal targets for employee awareness and their role in cyber defense.

Our approach

Given the scope of our operations and our contribution to energy infrastructure in North America, we take cybersecurity seriously. We work closely with government agencies in the U.S. and Canada (i.e., the Department of Homeland Security in the U.S. and the Department of National Defence in Canada), industry partners and peers to constantly monitor threats, evolve our cyber maturity and remain prepared to act.

Our systems and controls are tested annually by independent third parties through penetration/vulnerability assessments, as well as independent audits. We perform quarterly testing of cybersecurity incident response and recovery processes. Additionally, we assess our cybersecurity standards and test response and recovery capabilities on an annual basis. We monitor for potential threats and malicious activities across our environment around the clock through our Security Operations Centre.

Training

All Enbridge employees and contractors are required to take our Acceptable Use of Technology Assets training annually. The training describes how to safeguard our information and assets. The training also raises awareness regarding what actions to take to protect the Company when using technology assets and the internet. Additionally, targeted cybersecurity awareness trainings are conducted for higher risk groups within Enbridge, such as users with access to sensitive information. We add and update our training programs regularly.

Awareness

To elevate awareness of cybersecurity risks and responsibilities across the organization, our team shares information via emails, town halls and other special events, as well as through our intranet and social media. We transform emerging cybersecurity trends and topics into valuable learning experiences through our “Cyber Meeting Moments.” This internal repository features numerous presentation decks on cybersecurity topics and learning events, and is accessible to all employees. We also take part in external events such as industry working groups (e.g., American Gas Association, Interstate Natural Gas Association of America) and tabletops to learn and share.

Phishing

Phishing is one of the most prevalent cyber threats in our industry. Our phishing awareness efforts aim to educate employees to recognize the warning signs and report suspicious emails promptly. Our employees are expected to report any incident such as phishing or any other suspicious or malicious activity through our Security Operations Centre or our Enbridge Service Desk. We conduct simulated phishing tests every month to increase awareness and assess our vulnerability. We follow up with departments that are underperforming and provide additional support to employees who failed phishing tests via a web-based training course. We also perform targeted testing on high-risk groups and operational technology users (e.g., employees working at industrial sites).

More information

See our 2024 Sustainability Report for further information.