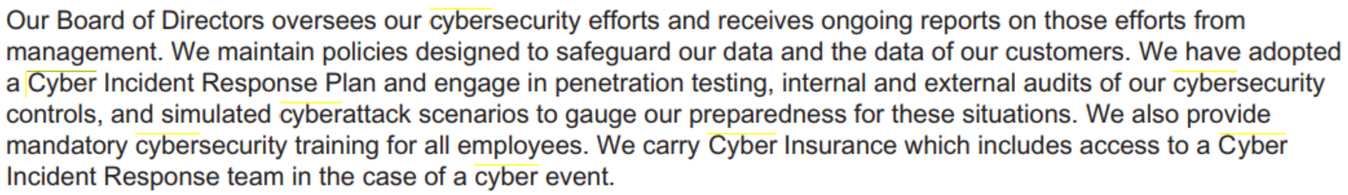
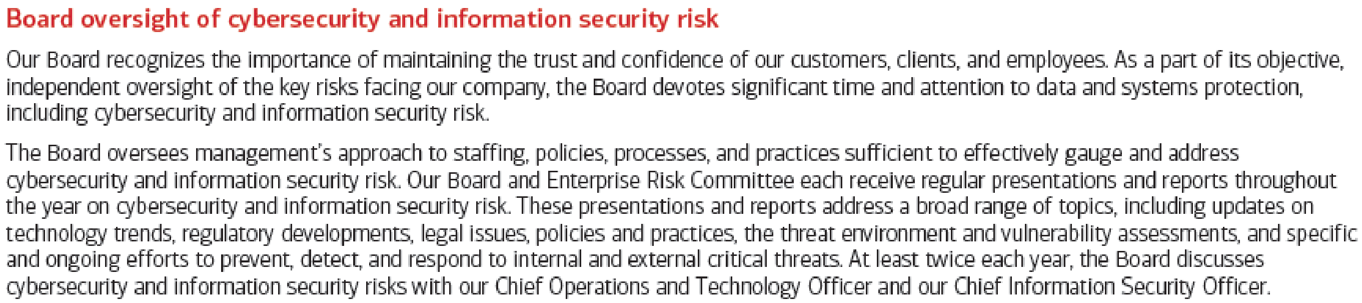
Disclosure Examples: Cyber Risk Oversight



Our Board of Directors oversees our cybersecurity efforts and receives ongoing reports on those efforts from management. We maintain policies designed to safeguard our data and the data of our customers. We have adopted a Cyber Incident Response Plan and engage in penetration testing, internal and external audits of our cybersecurity controls, and simulated cyberattack scenarios to gauge our preparedness for these situations. We also provide mandatory cybersecurity training for all employees. We carry Cyber Insurance which includes access to a Cyber Incident Response team in the case of a cyber event.

***

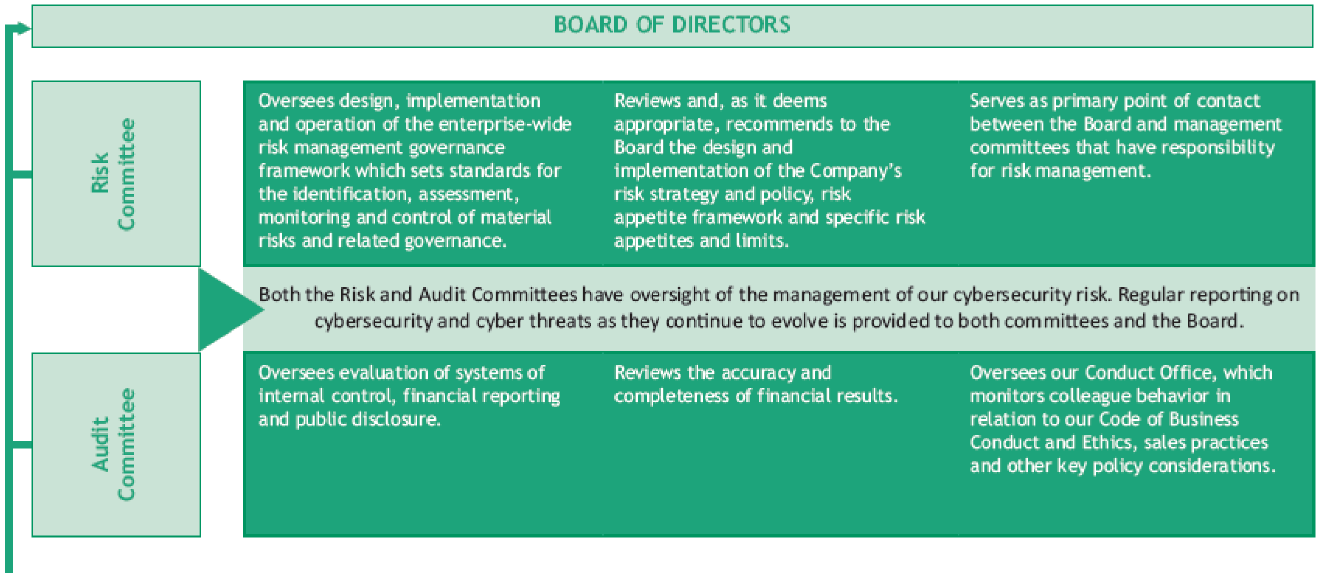


Board oversight of cybersecurity and information security risk

Our Board recognizes the importance of maintaining the trust and confidence of our customers, clients, and employees. As a part of its objective, independent oversight of the key risks facing our company, the Board devotes significant time and attention to data and systems protection, including cybersecurity and information security risk.

The Board oversees management's approach to staffing, policies, processes, and practices sufficient to effectively gauge and address cybersecurity and information security risk. Our Board and Enterprise Risk Committee each receive regular presentations and reports throughout the year on cybersecurity and information security risk. These presentations and reports address a broad range of topics, including updates on technology trends, regulatory developments, legal issues, policies and practices, the threat environment and vulnerability assessments, and specific and ongoing efforts to prevent, detect, and respond to internal and external critical threats. At least twice each year, the Board discusses cybersecurity and information security risks with our Chief Operations and Technology Officer and our Chief Information Security Officer.

***



BOARD OF DIRECTORS

Risk Committee

Oversees design, implementation and operation of the enterprise-wide risk management governance framework which sets standards for the identification, assessment, monitoring and control of material risks and related governance.

Reviews and, as it deems appropriate, recommends to the Board the design and implementation of the Company's risk strategy and policy, risk appetite framework and specific risk appetites and limits.

Serves as primary point of contact between the Board and management committees that have responsibility for risk management.

Both the Risk and Audit Committees have oversight of the management of our cybersecurity risk. Regular reporting on cybersecurity and cyber threats as they continue to evolve is provided to both committees and the Board.

Audit Committee

Oversees evaluation of systems of internal control, financial reporting and public disclosure.

Reviews the accuracy and completeness of financial results.

Oversees our Conduct Office, which monitors colleague behavior in relation to our Code of Business Conduct and Ethics, sales practices and other key policy considerations.

***

- **Cybersecurity Risks –** As a technology and communications company that enables global transmission of large amounts of information over our networks, maintaining the security and integrity of information and systems under our control is a priority among our operational risk management efforts. We view cybersecurity risk as an enterprise-wide risk, subject to control and monitoring at various levels of management throughout the Company. The Risk and Security Committee and its Chair review Cybersecurity and Data Privacy quarterly and such topics of review include:

  - risk assessments from information security, privacy and internal audit management teams with respect to cybersecurity, including the adequacy and effectiveness of the Company's internal controls regarding cybersecurity,
  - emerging cybersecurity developments and threats and
  - the Company's strategy to mitigate cybersecurity risks, such as our contingency plans in the event of security breaches or other system disruptions and cyber insurance coverage.

  To assess and mitigate cybersecurity risk, we have implemented a global information security management program that includes administrative, technical and physical safeguards and we periodically engage both internal and external auditors and consultants to assess and enhance our program, all of which is subject to oversight by and reporting to the Risk and Security Committee. We engage independent external auditors and consultants who are fully accredited under various information security standards, including those administered by the International Organization for Standardization and the PCI Security Council.