Information Technology and Cybersecurity Risk

Approach

Our approach to mitigating information technology and cybersecurity risk comprises a range of activities with the primary objective of maintaining the confidentiality, integrity and availability of information in our business. Although information systems are inherently vulnerable to interruption due to a variety of sources, we align our information system processes and controls with best practices as defined by the Center for Internet Security. We have invested in hardware, software, and personnel to provide endpoint protection, network firewalls, email protection, account management, system data backups, log auditing, data encryption, incident response, and system penetration testing.

Preventative Procedures

We regularly perform system reviews and security exercises to evaluate the effectiveness of our information security processes and controls. We work closely with accredited third-party cyber security firms to audit our security architecture and test our defenses. We invest in enhancing our preventive and defensive capabilities in line with information security standards, maintaining appropriate information security technology partners, and implementing other measures to mitigate potential threats and losses, where possible. To keep our employees mindful of information security, we require employees to complete annual information security and compliance training and regular phishing awareness exercises.

Board Oversight

Quarterly, we report to our Board of Directors on our information systems and cyber security initiatives, identified incidents, risk and compliance. Our Board has not delegated its information systems and cyber security oversight responsibilities to a committee; rather, these responsibilities reside at the full Board level.

Recent Experiences

Over the last three years, we have experienced no known information security breaches. Although we remain vigilant in our preventative efforts, cybersecurity incidents continue to expand in complexity and frequency, and we may be unable to prevent a significant incident in the future.

We did experience an immaterial breach during the fourth quarter of 2021, when we identified malware on our system resulting from a cyberattack. We successfully quarantined the malware without disruption to our operations. This quarantined breach required a rebuild of a triple-redundant server. While moving one of our critical systems to a newly rebuilt server, we experienced a server outage that resulted in approximately 1,700 flight cancellations in the fourth quarter of 2021. We estimated the impact of the outage negatively impacted our 2021 financial results by approximately $18 million (pre-tax). SkyWest's total revenue for 2021 was $2.7 billion for comparative purposes. We removed the malware from our system in the fourth quarter of 2021 and enhanced our preventative and detective processes to reduce the risk of a similar cyber-attack. We have not had a similar disruption event since the fourth quarter of 2021.