HASI Cybersecurity Program

Board Oversight of Cybersecurity

Cybersecurity and cyber resilience are pivotal functions in supporting our organization's responsibility to stakeholders to maintain profitable business operations.

In response to the dynamic global cyber risk environment, our Chief Technology Officer oversees the adaptation of cybersecurity and training programs, guided by the Finance and Risk Committee of our Board of Directors. The Chief Technology Officer leads our team of technology professionals responsible for the day-to-day execution of departmental efforts.

The governance of our information technology and cybersecurity program is jointly overseen by the Finance and Risk Committee of the Board of Directors and the Executive Leadership Team. The Chief Technology Officer provides quarterly updates on cybersecurity initiatives, including IT processes and regulatory compliance, to the Finance and Risk Committee of the Board of Directors at least every six months, unless otherwise urgent.

Cybersecurity Approach

Our focused cyber and information security strategy draws from operationally pragmatic components of the National Institute of Standards and Technology (NIST) Cybersecurity Common Standards Framework, Center for Internet Security (CIS) benchmarks as well as the Information Technology Infrastructure Library (ITIL).

Our cybersecurity infrastructure includes a combination of premier information technology services supported by proven vendors whose services address the range of risks identified by our Board's Finance and Risk Committee, internal risk management team and internal cybersecurity team.

Looking ahead, HASI plans to utilize a Governance Risk Compliance platform based on NIST and industry best practices, which allows us to evaluate our cyber risk preparedness year-over year. Through this approach, we also monitor that business partners and their subservice organizations are themselves following industry best practices. Based on findings from SOC 2 reports, we will evaluate the controls of a business partner to prove that each organization complies with audited cybersecurity controls. This approach is a significant step in the maturity of our cybersecurity program and positively differentiates HASI from both similar businesses of our size and also organizations much larger.

Culture of Cybersecurity Awareness

We instil cybersecurity awareness deeply within our company culture through comprehensive educational training for all employees. This training encompasses a mix of instructor-led sessions, quarterly modules, phishing identification courses, employee cyber-engagement events, and ongoing testing. These initiatives are designed to keep our entire organization well-informed about emerging threats, including social engineering attack vectors.

Our cybersecurity team treats every attempt to infiltrate our IT infrastructure with utmost seriousness, reporting attacks to authorities and relevant service providers when appropriate. We consistently assess the evolving threats and risks in the cybersecurity domain, enabling us to swiftly adjust our strategic approach and safeguard the essential day-to-day functions of our business.

Cybersecurity for Incident Response

Our cybersecurity incident response (CIR) strategy draws on a multi-layered security and backup strategy to redundantly protect our data and business assets from malicious cyber threats. Because maintaining operational continuity requires advanced protection against cyber risks, we regularly conduct cyber incident response training for leaders across all departments of the business.

Our incident response exercises employ cyber incident scenarios that require respective business departments to collaboratively devise responses in an operationally technical capacity. Cyber incident responses include developing a communication plan for the wider public, investors and business partners. Such cyber incident response drills familiarize staff with calculated, organization-wide countermeasures and instil the understanding that cyber risk response is a critical element in preserving stability and thus business continuity. This proven cyber risk mitigation ensures that our cybersecurity program evolves to proactively navigate and respond to the rapidly changing cyber risk landscape.

Proactive Cyber Risk Mitigation

We conduct ongoing vigilance toward mitigating cyber risks with an array of programmatic tactics. The Cybersecurity team consistently administers vulnerability analysis to ensure that any identified vulnerabilities are swiftly addressed and remediated accordingly.

Data Privacy

While privacy issues are the purview of both our IT and Legal departments, HASI does not collect Personal Identifiable Information (PII) from any visitors to HASI.com or our affiliate investor site. We have specific investor stipulations that preclude customers, business partners, and website visitors from providing us with PII. Our active effort to avoid collection and possession of external PII mitigates this ever-present cyber risk.

Typically, risk to PII is measured on the scale on which the company handles such information. Due to the nature of our business's digital presence, HASI places within a fraction of the smallest measurable PII risk scale.

In 2024, we reported zero data incidents affecting our network, business applications, customers or employees, including those involving Personal Identifiable Information (PII).

Business Continuity

Preserving business continuity amid a varied and changing world is of the utmost importance. HASI addresses business continuity hypotheticals by monitoring all business units' key processes to identify each's dependencies and vulnerabilities. While some of these dependencies and vulnerabilities by their very nature do not require technology solutions, ongoing conversations with individuals responsible for our ongoing profitable operation ensure that we adequately prepare for the unforeseen potential of any disruption.

HASI has developed Business Continuity and Disaster Recovery (BCDR) plans to manage its business units' ability to respond, recover, and continue operations in the event of an operational disaster, including the loss of critical systems and data. HASI validates these BCDR plans by performing tabletop exercises that walk through hypothetical scenarios and confirm teams are prepared for events that lead to business interruption. HASI IT reviews these plans periodically with relevant leaders and business units to validate and update plans.