Governance – Data Security

Overview

At Albany, data security and privacy are a top priority. Our business relationships are built on our stakeholders' confidence in and our transparency on our data security and privacy policies. We care deeply about protecting personal and confidential information of our customers, employees, vendors, partners, and others, so all our stakeholders feel safe to do business with us.

Our Data Security strategy is built around four core pillars: **cyber security governance and accountability, industry best practices, technological standards and frameworks**, and **awareness and training**. Our policies are embedded at the core levels of our corporate structure to ensure accountability and efficient, fast processes.

Our strategy is governed by the Audit Committee of our Board of Directors, led by our Director of Information & Cyber Security, who leads Albany's Enterprise Cyber Security (ECS) team. To protect our company and customer data, our strategy calls for adhering to the newest security technology frameworks and standards, such as CIS20 and NIST SP800-171, released and updated by official entities. Additionally, we employ industry best practices, such as employee-wide cyber security training. Together, these pillars enable us to continuously improve our process of collecting, storing, processing, and distributing data safely and are consistent with the regulations of countries in which we do business.

Pillar #1 — Enterprise Cyber Security Governance & Accountability

By deeply embedding our data strategy within our organization, and establishing reporting lines, times, and accountability at the leadership level, we ensure our data security and privacy strategy remains a priority for us at all times.

To ensure the availability, confidentiality and integrity of information systems and data across all lines of business and locations, we established an internal Enterprise Cyber Security (ECS) team that is globally accountable. Our ECS team is directly managed by our Director of Information & Cyber Security within the Global Information Services (GIS) organization reporting to the Chief Information Officer (CIO). The ECS is supported by other key GIS teams who work collaboratively with global business units and corporate functions to continuously improve our cybersecurity posture.

Board Oversight & Risk Management

The ECS Team has direct input into the Enterprise Risk Management (ERM) process managed by the Corporate Chief Financial Officer. The CIO and VP of Information Technology (IT) have permanent seats on the ERM steering committee and are responsible for identifying and mitigating cyber and data security risks. Progress on cyber risk mitigation is presented quarterly both to Albany Leadership and the Audit Committee of our Board of Directors via the ERM.

Supported by multiple functions, the VP of IT is accountable to implement the broad range of risk assessment, infrastructure security services, threat and vulnerability management, business continuity, and compliance and policy management within Albany. On a bi-annual basis, our CIO reviews status of cybersecurity-related risks – such as business interruption, data loss, and financial funds loss – directly with the Audit Committee.

Enterprise Cyber Security Team Goal & Mission

The ECS team offers technical expertise to manage IT risks in Albany's initiatives and operations as well as enable corporate growth and information sharing in a secure manner to support the business. ECS ensures IT regulatory compliance and defines a governance strategy to safeguard Albany information assets against misuse, damage, and unauthorized access while empowering Albany employees to be security-minded and aware.

Protecting and monitoring our global IT footprint are core day to day functions of the ECS Team. Our ECS team and its mission are embedded in the acquisition, implementation, and management of our internal and cloud-based IT solutions at Albany.

Security Architecture & Operations

The ECS team works intimately with Albany's other Enterprise teams in the cross-disciplinary mapping of corporate business strategies and environmental conditions while leveraging internal expertise, industry best practices, and lessons learned. This mapping is translated into cyber security requirements, recommendations, designs and architectural roadmaps to maintain a relevant, efficient, and effective security posture throughout the organization. The overarching principle of the cohesive work relationship allows Information Security to become an integral component of Albany's Global Information Systems with security designed into the process from the onset.

Pillar #2 – Applying Cyber Security Best Practices

Threat Intelligence

The ECS team is responsible for conducting current and emerging cyber threat research to maintain an understanding of cyber-related threats and related criminal activities specific to our company. This work is supported by various IT solution providers and other third-party vendor consulting, monitoring, and threat intelligence subscriptions. Additionally, we maintain close relationships with relevant law enforcement and regulatory bodies.

Protection, Detection & Monitoring

Following our external frameworks and industry best practices, Albany maintains an evolving defense-in-depth strategy that relies on multiple related technologies and processes.

Albany maintains both a centralized automated patching process and a robust vulnerability assessment program in which servers, client PCs, infrastructure, and network appliances are prioritized and scanned, both actively and passively, on a regular basis. Devices and software found vulnerable are addressed through Albany's standard IT service management processes.

We also regularly engage external parties to conduct external assessments on specific and current cybersecurity risks. These assessments include network penetration tests, ransomware simulations, industrial controls security evaluations, and numerous others.

Cyber Incident Response Team

When an incident is reported or detected, ECS manages our Cyber Incident Response Team (CIRT). The CIRT process is overseen by and has direct participation of Albany's leadership team. Among the responsibilities of the CIRT is to respond to data breach incidents.

ECS manages the Albany Cyber Incident Response Team (CIRT). The role of the CIRT includes executing and coordinating incident response activities, as well as performing several other security and incident response related functions, all with the goal of minimizing the overall risk to Albany information and IT assets.

If the CIRT identifies a reportable or impacting security incident, a rapid summary of the situation is provided directly to senior leadership including the Albany CIO and General Counsel, who make determinations about impact and required communications to internal stakeholders, as well as external parties such as customers, vendors, and law enforcement.

Pillar #3 — Cyber Security Standards & Frameworks

Albany has adopted and adheres to frameworks for assessing and guiding cybersecurity preparedness including the CIS 20 and NIST SP800-171 to prevent and stop dangerous security threats from known attack vendors and protect our critical infrastructure. Both frameworks are reviewed quarterly, and gap assessments are conducted. Ongoing alignment and cyber risk maturity measurements are presented quarterly to our Senior Management and to ERM steering committees. Additionally, beginning in 2020, we began implementing the United States Department of Defense Cybersecurity Maturity Model Certification (CMMC) requirements specifically for our defense-related business.

Albany International is Sarbanes-Oxley (SOX) compliant, our website, Albint.com, is CCPA compliant, and our Data Governance Programs include Europe's General Data Privacy Regulation, and US Government classifications including EAR / ITAR / CUI.

Pillar #4 - Cyber Security Awareness & Training

Supporting ECS efforts is a comprehensive suite of cybersecurity, data protection, and privacy training conducted annually for all our employees. The objective of the ECS Security Awareness and Education Program is to increase the overall security knowledge of the end user, reduce high risk activities through education, highlight security policies, develop up to date training, and provide notification of current threats. Our training is continuously adapted to the evolving risks and regulations of our global markets. Email phishing awareness training also is conducted annually for all employees with an email address, and phishing simulation tests are conducted throughout the year with additional training and retests required for all failures.

SASB Data Security Disclosures:

Albany International is categorized in the Industrial Machinery & Goods industry under the SASB's Sustainable Industry Classification System® (SICS®) and discloses information and data to that standard. Given the company's significant aerospace composites business, the company has elected to supplement its disclosure by reporting certain relevant Sustainability Disclosure Topics and Accounting Metrics contained in the SASB Aerospace & Defense standard. The reporting boundaries for the disclosure metrics below include all parent and consolidated subordinate entities of Albany International Corp.

DATA SECURITY

SASB CODE	ACCOUNTING METRIC	CATEGORY	UNIT OR MEASURE	DISCLOSURE	
				2020	2019
RT-AE-230a.1	(1) Number of data breaches	Quantitative	Number	None	None
	(2) Percentage involving confidential information	Quantitative	Percentage	0%	0%
RT-AE-230a.2	Description of approach to identifying and addressing data security risks in	Discussion and Analysis			
	(1) company operations			See discussion above	
	(2) products			Not Applicable: Albany International does not produce or sell products containing any data collection or processing capability.	