Cybersecurity Risk and Oversight

At Hexcel, we are committed to the security of our products, services, and data. We recognize that at any time, the Company may be the target of attempted cyber attacks and other security threats. Therefore, we constantly improve our systems and processes that predict and protect our capability to keep pace with the evolving threat landscape. In addition, we continuously monitor and audit our information technology and data assets to detect any anomalies and to respond quickly to threats that may arise.

Risks

Cyber risks for our business and manufacturing capability may include:

- An unauthorized disclosure of sensitive or confidential Hexcel, customer or employee information by individuals or as a result of a cyberattack. Such a disclosure could cause a loss of data and give rise to remediation or other expenses, including exposure to liability under U.S. federal and state laws, as well as non-U.S. data privacy regulations. Investigations and litigation in such a scenario could have an adverse effect on our business, cash flows, financial condition and results of operations.
- The theft of our intellectual property for the benefit of domestic or foreign aerospace and defense competitors, and the development of technologies for sale in global markets to unauthorized third parties.
- A disruption to our manufacturing capability through a targeted attack intended to stop production or damage production equipment.
- A disruption to normal business operations by impacting supporting IT services and applications.
- Disruption of normal business operations due to a failure of services procured from third-party suppliers who themselves come under a cyberattack.

Hexcel is compliant with the National Institute of Standards and Technology (NIST) 800-171 standard for the protection of controlled unclassified information.

Response

Hexcel has established a framework for decisions and actions at the executive level to contain and recover from cybersecurity incidents. Each cyber incident is unique. Our response, though it should follow defined protocols, must also adapt to each incident as it occurs. With that in mind, we have established several protocols within a structured approach to guide leadership and the company through an active threat or incident to the recovery of normal business. These protocols follow leading data protection standards.

Hexcel has adopted a four-quadrant approach to cybersecurity management – Predict, Block/prevent, Detect, and Respond. We use various tools and processes to predict and detect passive or directed attempts to compromise Hexcel data, systems, or business capability. Each occurrence, whether generated from an outside or internal source, is considered an event and is captured by the Hexcel IT Technical team and followed to a conclusion.

Hexcel is committed to notifying appropriate stakeholders should a data breach or significant threat to business operations occur. Hexcel categorizes cyber incidents by their potential impact to employees, customers, and its business. Each incident includes a written protocol for rapidly notifying those parties who are or are potentially impacted by the incident, as well as those who have the capability to contain and remedy the incident.

Investigations

Hexcel investigates all credible reports of security vulnerabilities affecting our organization. We continue to evolve our security policies, procedures, and capabilities to ensure appropriate management of security incidents. The Company, as required by law or regulation, will make timely disclosures of any related material information and cyber risk.

Governance

Hexcel has an Executive Response Team that is trained and experienced in managing cyber incidents. This team – which includes the Company's most senior leaders in various functions – meets at least twice a year to practice and refine the Company's process to respond to, manage, and escalate incidents. The Team will be called to respond each time a cyber incident exceeds a specific impact level.

Our Board of Directors views cybersecurity as a strategic risk issue and therefore maintains close oversight of management's actions in implementing our overall cyber risk management strategy and policies.

Training and Communications

Hexcel believes a well-trained and informed workforce is key to maintaining a secure IT environment. We provide employee awareness training on email management (phishing), safe internet browsing, malware, and other cyber risks to ensure that the Company is protected, to the greatest extent possible, against cyber risks and security breaches. We routinely communicate with employees about the potential for cyber threats and how to avoid them through our established communications channels. In addition, we regularly "audit" our employees' ability to recognize security threats. Those who do not respond appropriately receive additional training and may be subject to discipline.

Updated: November 2020