Cybersecurity risks

Scenario and Risk Assessment:

Changes in work patterns and business operations to be more reliant on technology such as work from home during the COVID-19 outbreak and digital workplace that allows employees to connect, communicate, and work together through various channels and devices; the adoption of digital technologies in the industry such as mechanization, automation, and robotics; and the implementation of other digital technologies to increase business efficiency in every step from production through to product delivery to customers could pose various types of cybersecurity threats. These include data spills or leakages and cyberattacks on critical infrastructure and production processes.

Impact:

These adversaries could result in loss of the Company's critical information such as product and development information and trade secrets, as well as personal information of customers, business partners, and employees which could tarnish the Company's reputation and credibility. Other potential impacts could be financial damages from paying ransom for ransomware attacks, litigation and regulatory fines, or losing revenue or profit as a consequence of failing to maintain cybersecurity vigilance.

Mitigating Action and How to Convert to Opportunities:

SCG has defined cybersecurity risk management measures as follows:

· Appointed SCG IT Governance Committee (ITG) and The Cybersecurity Governance Committee to establish policies and regulations on the use of information and communication technology (SCG e-Policy) for all SCG employees to adhere to in a consistent manner and oversee SCG's information technology security practices and ensure that they are aligned with business directions and can effectively prevent business operations from cyber threats. The ITG is chaired by Mr. Yuttana Jiamtragan who is Vice President-Corporate Administration, member of digital council committee, and SCG Executive Management team, has role and responsibility in overseeing the IT, cybersecurity, data privacy, startup, and digital innovation with his skill and expertise in IT and information security as well as digitalization.

· Established SCG e-Policy in alignment with the ISO 27001 international standard and developed cybersecurity plan that encompasses usage and measures to prevent cyber threats for domestic and oversea companies under SCG. Chief among them are data classification and management, guidelines for using social media effectively, and regulations on information technology use for employees involved with human resources.

- Continuously promotes awareness on use of technology among employees through various trainings and other activities to ensure employees have knowledge and understanding on effective use of technology and to protect business from cyber threats. A test on employee awareness and understanding about the SCG e-Policy is also organized on an annual basis.
- Installed Web Application Firewall to increase data security and reduce risks from cyber attacks.
- Assesses cybersecurity risks on industrial control systems and implemented risk mitigation measures by both the Company's internal functions and third parties.
- Developed Disaster Recovery Plan (DRP) to handle emergency, enabling users to continue working through a backup site. The Cyber Incident Response Plan was also put into place and regularly drills are carried out to prevent business interruption from cyber attacks.

Source: 2020 SCG Annual Report (Page 73 – 74)
(https://scc.listedcompany.com/misc/one-report/20210305-scc-one-report2020-en.pdf)