Data Privacy & Cybersecurity

Related UNSDGs:

WHY IS THIS IMPORTANT?

Our mission explicitly outlines our emphasis on utilising technology to enhance efficiency and gain a competitive advantage through innovative approaches to deliver value for an improved quality of life for our identified stakeholders.

As a Group, we acknowledge that leveraging digitalisation is the most effective approach to connect with our stakeholders and optimise the efficiency of our operations. This acknowledgment is emphasised in our IAP 2.0, where digitalisation is identified as a critical success factor for our ongoing progress.

However, the Group also recognises the paramount importance of ensuring data privacy and safeguarding against potential hacking threats. Weak protection of our data not only disrupts operations but also poses reputational risks among our stakeholders. This lack of security may erode trust in the Group, ultimately affecting confidence in future business engagements.

OUR APPROACH

The Group reinforces its cybersecurity protocols by adhering to our Information Technology Acceptance Use Policy. This policy is applicable to employees, contractors, consultants, temporary staff, and other affiliated third parties within the Group. It explicitly outlines the proper utilisation of information, electronic devices, computing devices, and network resources when conducting business for the PB group of companies. This includes interactions with internal networks and business systems, whether owned or leased by the PB group of companies, the employees, or a third party.

Adhering to the fundamental tenets of effective corporate governance and in accordance with the guidelines outlined in Practice 10.1 of the MCCG 2021, our Board oversees cybersecurity incidents and related issues under sustainability agenda through KPIs reported through its BRMC. Besides setting KPI and monitoring it, the Board assesses critical risk associated to cybersecurity, and ensures the Group implements measures to alleviate or address those risks. While the present objective is to conduct a minimum of one awareness session for all employees on cybersecurity, the severity and impact of cybersecurity incidents will be highlighted for better understanding.

In FY2023, the following measures were implemented to address data privacy and cybersecurity issues:

a. The implementation of Sangfor firewall on all company-owned computers and personal laptops connected to the company servers is currently in progress.

b. An audit was conducted on each computer utilised by employees to detect any cybersecurity risks. This process is ongoing, with further comprehensive actions planned for the future.

OUR PERFORMANCE

As of FY2023, there were 17 substantiated complaints concerning cybersecurity. However, no breaches in customer privacy or data loss have been reported.

Details	FY2023	FY2022	FY2021
Number of incidents of cyber attacks	**17**	N/A	N/A
Number of users affected by data breach(es)	**0**	N/A	N/A
Number of cybersecurity awareness and other related programmes	**1**	1	N/A