5.4 Cybersecurity and Information Technology Policy

The company prioritizes and recognizes the importance of managing risks, maintaining cybersecurity and information technology systems to prevent risk levels and prepare for threats.

The Risk Management and Monitoring Committee and a technical issue consideration team have been appointed. The company assesses its Cybersecurity Maturity based on the National Institute of Standards and Technology (NIST) framework to ensure confidence and security for customers and stakeholders comprehensively.

Actions are driven to align with the cybersecurity and information technology policy, which must be strictly complied.

Guidelines for managing risks to data security and information systems

The Company has established systematic and effective guidelines for managing and controlling information security and information system risks, adhering to principles and practices aligned with international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework, in order to strengthen the security of data and information systems. This ensures the Company is well-prepared to plan, prevent, detect, and respond to various threats in a timely, systematic, and highly effective manner.

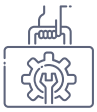
These guidelines are aimed at strengthening the security of data and information systems while ensuring readiness to plan, prevent, detect, and respond to potential threats in a timely, systematic, and effective manner. The Company operates in accordance with the following approaches:

Governance:

Information technology security and stability.

Self-Assessment:

Evaluating the capability to manage IT security and stability.



Planning and Improvement:

Continuously reviewing the IT security and safety policy.

Awareness and Preparedness:

Continuously raising awareness and preparing all employees and partners for cybersecurity.

Monitoring and Risk Assessment:

Monitoring operational outcomes, using strategies and measures to reduce the risk or mitigate damage.

Governance of Information Technology Security and Safety

The Company has announced and reviewed its cybersecurity and information technology system policies, taking into consideration relevant legal requirements as well as stakeholder expectations, in order to establish appropriate directions, principles, and operational frameworks for information security.

Furthermore, the Company has appointed a Risk Management Oversight Committee and established a technical working group, with the Information Technology Department serving as the primary responsible unit for monitoring operations and regularly reporting results to the relevant committees. The full policy document is available for download at:

https://www.satpcl.co.th/storage/content/sd/disclosure-documents/20230328-sat-policy-cyber-security-and-it-systems-th.pdf

Self-understanding through the assessment of capabilities in managing information technology security and safety.

The Company participated in the Cyber Resilience Survey 2025, conducted by the Stock Exchange of Thailand in 2025, and also carried out assessments related to key customers, referencing the internationally recognized NIST Cybersecurity Framework under both Version 1 and Version 2, in order to determine the level of capability in managing information technology security. The assessment results are utilized for continuous improvement of policies, operational planning, and development, to sustainably maintain its position as a leading company in the industry under efficient and appropriate resource management.

Planning and improving information technology security policies

The company plans to control and oversee the information technology system, along with improving processes related to information technology security and data protection. This includes data analysis enhancement and extending the scope to cover all companies in the group, including subsidiaries, to ensure that the systems meet the appropriate standards. The preventive plans are as follows:

Improvement

Review the Business Continuity Plan (BCP).

Supply Chain Risk Management

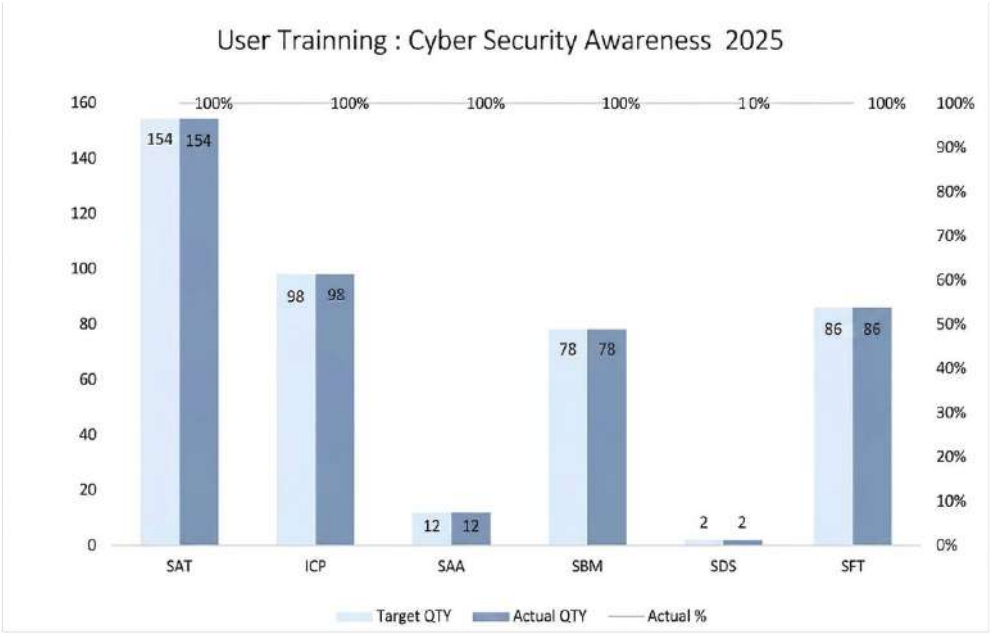
Conduct joint BCP drills with relevant partners.

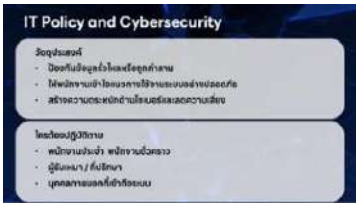
Analysis

Improve procedures for analyzing cybersecurity incidents upon receiving alerts.

Promoting awareness of the information technology security policy

The Company places importance on developing employees' knowledge and awareness of cybersecurity and safe use of information technology systems by providing continuous training, communication, and learning through a self-learning system, covering employees at all levels, including new employees.



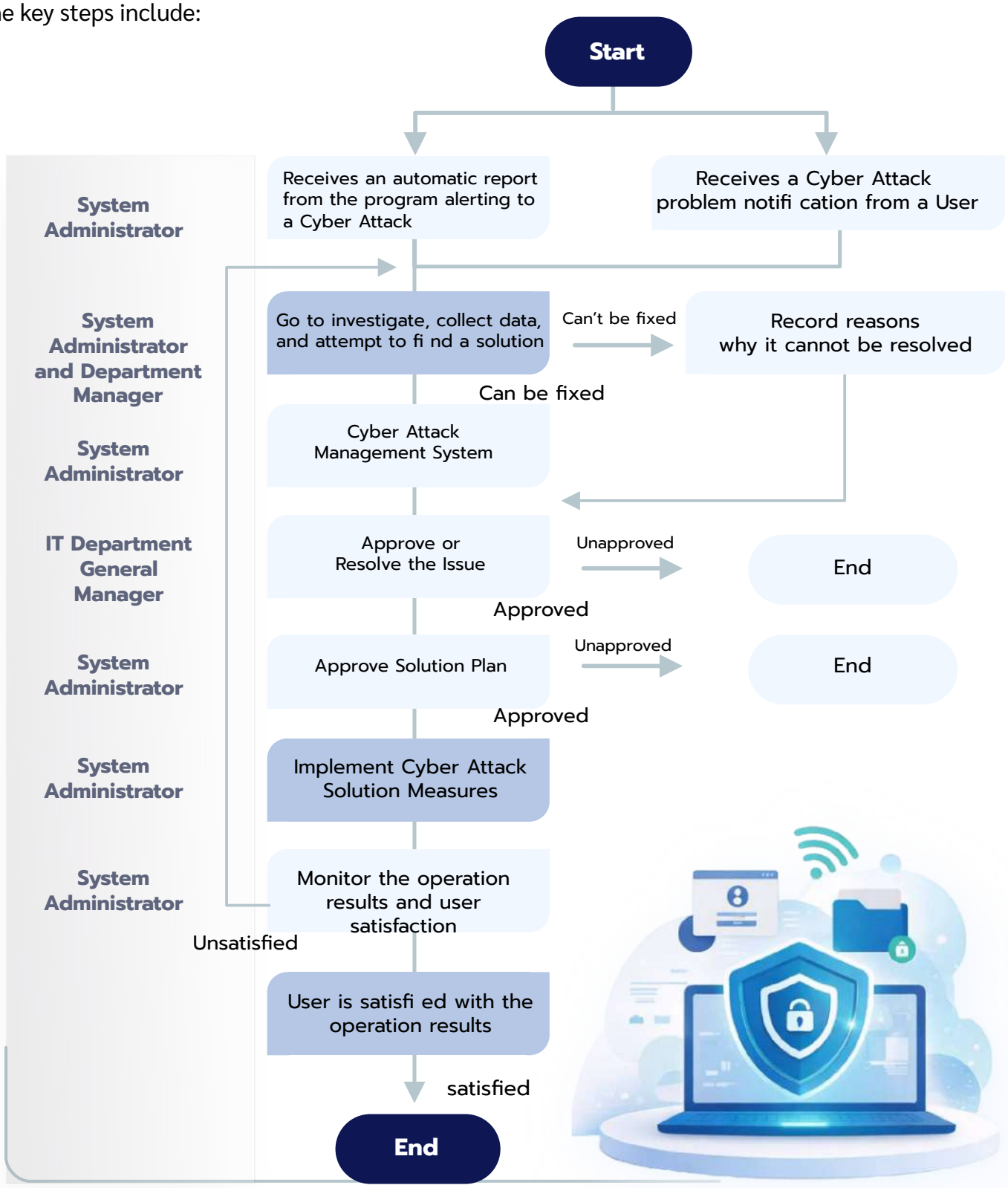


Continuous monitoring and risk assessment

Currently, the Information Technology department has conducted risk assessments with key risk indicators for evaluation, reporting to the organization-level risk committee monthly. This ensures effective risk management and minimizes potential impacts on the organization and business opportunities.

Handling Complaints and Responding to Cybersecurity and Information Technology Incidents

The company has established a system for managing complaints regarding information technology security, accessible through a web application, email, and telephone. Employees can contact the complaint recipient around the clock via telephone or email through the Helpdesk system, an internal company web application, or at cybersecurity@somboon.co.th. The key steps include:

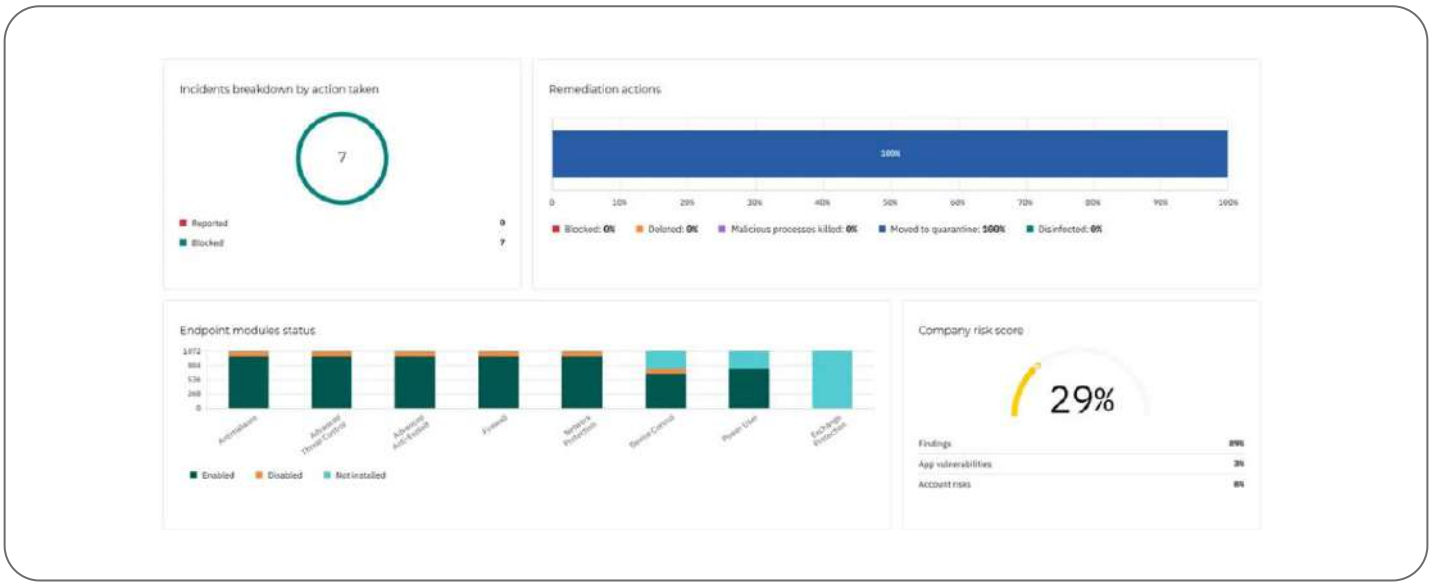


Performance Result of IT and Data Security in 2025

The Organization's Preventive Computer Virus Capability for 2025

Month	No of Attacks	No of Preventions	No of Successful Incidents
January	573	573	0
February	575	575	0
March	620	620	0
April	569	569	0
May	615	615	0
June	663	663	0
July	744	744	0
August	608	608	0
September	654	654	0
October	659	659	0
November	649	649	0
December	916	916	0
Total	7,845	7,845	0

Prevention Measures



- Implemented a backup server system for authentication and authorization of devices accessing the internal network via the cloud.
- Achieved 100% protection against computer virus attacks.

performance 2025

1. Project to Upgrade ERP-SAP ECC เป็น ERP-SAP S/4 HANA (Effective from 2 May 2025)

2. Prevented 100% of attacks from computer viruses

3. Deployment of a Two-Factor Authentication (2FA) Security System

4. None of interrupted business continuity incidents arising from cybersecurity risk

5. The SAP-ERP system vulnerability test has been validated by an independent audit company.

6. Provided 100% of cybersecurity and information system trainings to new employees using computers.