Cyber Security Management

Excerpted from P.106~P.108 of the 2022 Annual Report

VII. Cyber security management

(I) Cyber security risk management framework, policy, specific management plans, and resources put in cyber security management

1. Cyber security risk and management

- The scope and purpose of cyber security

  Parties/Entities concerned: Employees, clients, suppliers and shareholders, as well as operation-related information software and hardware equipment.

  Scope: To ensure the Company's information security, we formulated rules and regulations, adopted technology and data security standards, and incorporated them into the management and operations system to protect employees', suppliers', and clients' privacy and information security during business dealings.

■ Cyber security risk management framework

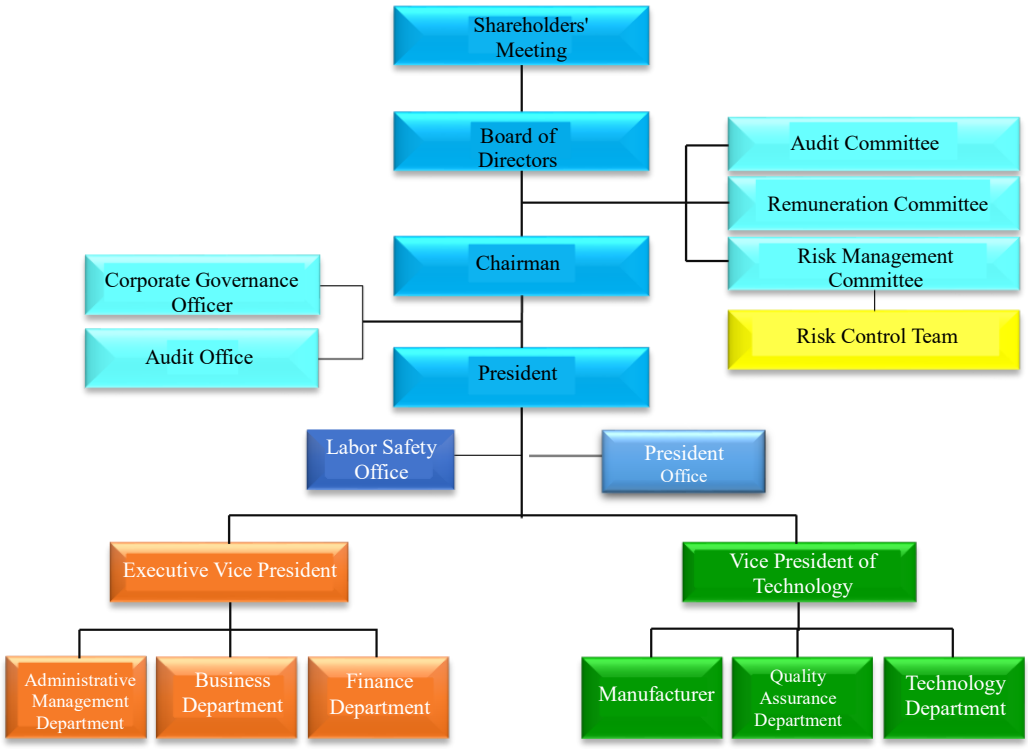
To enhance the Company's stable operation and sustainable development, establish a complete risk management mechanism, and reasonably ensure that we achieve the Company's strategic goals, we have established a Risk Management Committee and formulated risk management policies and procedures in accordance with Article 27 of the Corporate Governance Best Practice Principles for TWSE/TPEX Listed Companies.

The Risk Management Committee assists the board in fulfilling its risk management responsibilities and is responsible for reviewing various risk management issues. A Risk Management Task Force is set up under the Risk Management Committee to assist the committee in fulfilling its risk management responsibilities. The Risk Management Committee meets at least twice per year and reports to the board at least once a year.

The executive secretary of the task force is served by a first-line manager at the Administrative Management Department, and the members of the task force are the middle managers or above at each plant's departments. The task force is responsible for the overall risk management, including operational, financial, information security, environmental, compliance, and other risks.

Among them, information security risk management is conducted by the Information Section, Administrative Management Department. The section comprehensively manages the Company's information strategy

planning, implementation, and management, optimizes the information system structure, enhances information management efficiency, and implements and regularly reviews and modifies information security systems and management measures.



2. Cyber security policy objectives

- Control information security risks, strengthen prevention, reinforce the information security structure and internal control, and ensure proper protection of information assets.
- Establish a complete management system to ensure the confidentiality and integrity of information assets.
- Establish an up-to-standard information security mechanism and regularly review and amend relevant operating regulations to comply with cyber security standards.
- Be commitment to integrating and managing all potential risks that may affect information security in proactive and cost-effective methods.

3. Specific cyber security management plans

- Regularly assess the impact of man-made and natural disasters on the Company's information assets and formulate a recovery plan to ensure business continuity.
- All employees of the Company as well as clients and suppliers who use or link with the Company's domain or computer systems should abide by the Company's information security regulations as required.
- Regularly offer internal information security and information system training courses and require information personnel to actively participate in information security seminars to enhance their professional skills.
- Regularly raise personnel’ s awareness of information security policies and

offer information security education and training to increase employees' awareness of information security.

- Announce any external major information security incidents by email and on the homepage of the Company's website, to remind employees of various types of information security threats and new threats to enhance their awareness of information security.
- Enhance information security, prevent the leaks of trade secrets, and manage permissions for user accounts, changes of VPN firewall connection rules, USB/storage devices, and visitors' use of domains.
- Regularly carry out relevant backup protection measures for the information system structure, such as off-site host backup, cloud, and on-premises data backup, and power backup; test the restoration of backup data and the backup power system per month; inspect and update the operating systems in real time to ensure the normal operations of the information systems and the reliability of data retained.
- In accordance with the above policies, we regularly monitor subsidiaries' potential information security risks timely and take active measures to reduce potential harms.

4. Implementation of information security risk management

We held two Risk Management Committee meetings and two meetings of the Risk Management Task Force during 2022 to review each unit' s implementation of the information security policies; they reported to the Board of Directors in 2022. No incident that undermined information security occurred during the year. According to the "Guidelines Governing the Establishment of Internal Control Systems in TWSE/TPEx Listed Companies", in November 2022, a dedicated information security supervisor and qualified personnel were put in place, thus being implemented one year earlier than required.

▼Resources invested in cyber security management

Management countermeasures	Execution instructions
Replacement of one mainframe server	■Avoid the possibility of system crashes due to outdated equipment. ■The replaced server is converted to a terminal for use, maximizing the residual value of the server and increasing the smoothness of on-site operations.
Replacement of two on-site network switches in Building B	■The device has been in use for 15 years and has no network management function for active/passive defense management in case of anomalies, which is extremely risky. ■The above-mentioned defensive functions were enhanced after the replacement to reduce information security risks.
Growth rate of external network mergers	■The increased demand for video conferencing as a result of the epidemic has led to a lack of network bandwidth, which has affected the quality of meetings; and an increase in the frequency of network traffic attacks has increased the threat

	to the company's network. ■The original company used three external 100/40 mb/s enterprise networks, abolishing one and increasing the speed of two from the original 100/40 mb/s to 300/100 mb/s; the total input cost increased by 10.5%, but the total bandwidth download growth rate was 300%, and the upload growth rate was 160%, resulting in a significant increase in efficiency. ■Telecom offers free traffic attack cleaning service. Compared with August, the number of abnormal traffic attacks in July dropped from 14,427 in the previous month to 1,365, representing a 90.54% reduction, effectively reducing the load on the Company's network firewall equipment, as well as the chance of external network failure and firewall failure after an attack.
Strengthen colleagues' awareness of information security	■Monthly information case awareness-raising events are conducted to raise prevention awareness among colleagues. ■Conducting internal penetration test: In addition to the reflection paper, colleagues who have been successfully penetrated are required to prepare a specific information security topic for the Company's staff to enhance their awareness of the need to prevent being hacked.

5. Information security training and awareness-raising events:

In 2022, a cumulative total of 12 information security awareness-raising events per month was conducted; in July, a total of 10 people (including the subsidiary) were successfully penetrated during two information security awareness-raising events, and in September, a total of 117 participants attended nine training sessions over three days to raise awareness on information security among colleagues; the subsidiary held a training session on 13 October in the same manner as the parent company, with a total of 20 participants.

▼Internal and external education training and awareness-raising events are listed below:

Internal/External training	Category of course	Number of people	Number of hours/people
External training	D Webinar 2022 Digital Transformation Forum - New Work Models	3	6
External training	Information security and Seminar - Aruba Networking Future Innovation Technology Online Seminar	4	2
External training	Why is cloud data backup so important to small businesses?	3	2
External training	Online seminar bringing together experts from Dell Technologies, Intel and VMware	3	2
External training	Seminar on New Key Factors for Enterprise Victory	3	2
External training	Intelligent manufacturing transformation and comprehensive anti hacker measures, no longer blurring the boundaries of IT/OT	4	8
External training	Cloud Intelligence for SMEs - Easy Network Management	2	2
External training	SecurityTRENDs 2022	1	4
External training	AWS ESG Digital Transformation Summit for the	1	4

	Manufacturing Industry		
External training	A new cloud landscape for post-epidemic sustainability	4	2
External training	Cyber Security Maturity Compliance (CMMC) Seminar	1	4
Internal training	2022 Information Security Education and Training -1	24	2
Internal training	2022 Information Security Education and Training -2	2016	2
Internal training	2022 Information Security Education and Training -3	115	2
Internal training	2022 Information Security Education and Training - Subsidiary	20	1
Internal training	Firewall and hack prevention training for information courses	4	8
Awareness-raising events	13 internal awareness-raising event on information security		

(II) Specify the losses incurred due to major cyber security incidents, potential impacts, and countermeasures in the most recent year and up to the publication date of this annual report. If the amount cannot be reasonably estimated, please specify the fact that it cannot be reasonably estimated: N/A.