Cyber Security Management

Excerpted from P.111~113 the 2023Annual 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.

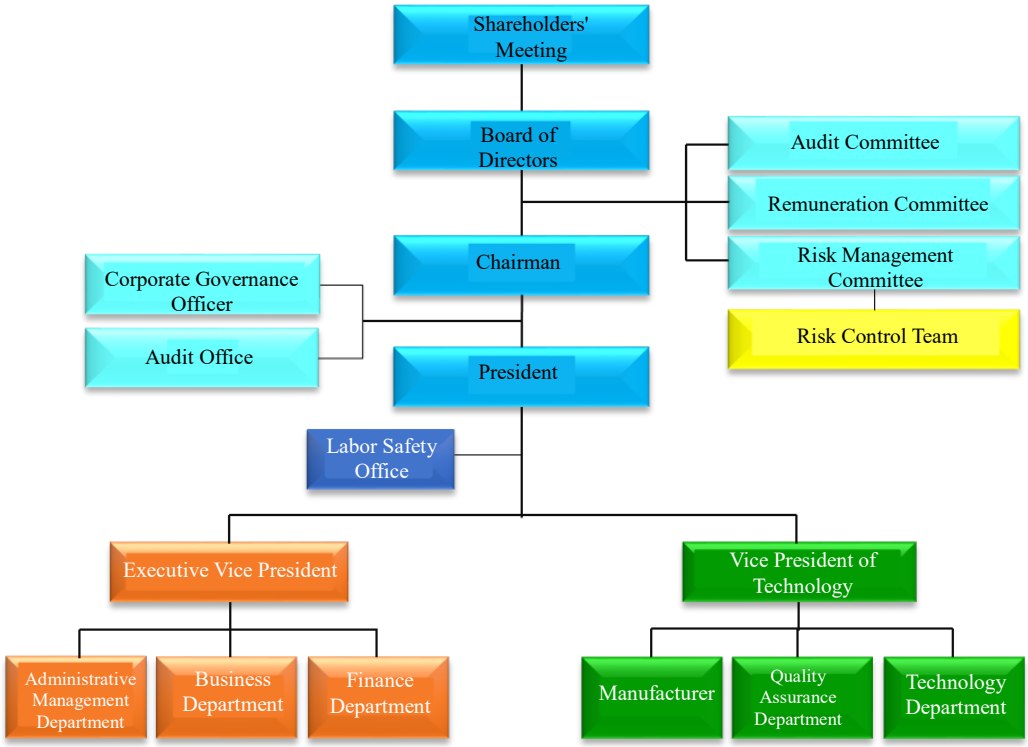
■ Cyber security risk management framework

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 2023 to review each unit' s implementation of the information security policies; they reported to the Board of Directors on November 2, 2023. 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
Upgrade business machine authentication and record management system	■The current core network switches are more than 10 years old and cannot handle the current company's network traffic. They have been compiled for the past three years and were originally intended to be replaced year by year. However, they were stopped due to the progress of the 5G AIOT project. This year's core switches If a malfunction occurs, repair is required. The original factory no longer supports maintenance and replacement is urgently needed. ■The worry of no warning failure after replacement has been solved..
There are 4 core network switches in Building AB	■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.
Update an HP SERVER	■The company has been replacing servers that have been used for more than 8 years. One server was updated last year, and the remaining one needs to be updated to ensure the stability of the above operating system. ■After the replacement, the system stability is improved to avoid system failures and reduce information security risks.
Surveillance system software replacement	■The original system is no longer maintained by the original factory, and system vulnerabilities cannot be patched. At the same time, it does not support new operating systems, which increases the risk of being hacked. ■After the update, the above problems have been solved and the risk of being hacked has been reduced.
Network Load Balancer Update	■The function of this device is to disperse the company's external network traffic and avoid congestion. It has been used for more than 10 years. It has crashed several times and needs to be replaced. When the failure occurs, all networks will be unable to connect to the outside world. At the same time, the original factory of the system is no longer maintained. There may be concerns about subsequent vulnerability patching and information security issues. ■The above problems have been solved after replacement.

Develop information security management system	■As there are a certain number of systems and devices that need to be managed and they are scattered on different systems, management becomes more difficult. In order to achieve effective management, this system was developed to improve visibility and prevent in advance through a single platform and interface. ■The development is currently going smoothly and is expected to be completed by the end of 2024.
Strengthen colleagues' information security awareness	■Promote information case examples every month to enhance colleagues' prevention awareness. ■Conduct internal penetration testing: In addition to reporting on their experiences, colleagues who have been successfully penetrated need to prepare a specific information security topic for company colleagues to teach colleagues to increase their vigilance and prevent being hacked.

5. Information security training and awareness-raising events:

In 2023, a cumulative total of 15 information security awareness-raising events per month was conducted; a total of 2 people (including the subsidiary) were successfully penetrated during two information security awareness-raising events, and in September, a total of 79 participants attended nine training sessions over three days to raise awareness on information security among colleagues; thus effectively improving employees' security awareness, the successful penetration rate has dropped from 3.6% to 1.8% year by year.
The subsidiary held a training session in the same manner as the parent company, with a total of 19 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	Smart network. New Thinking in Security Management Seminar	1	8
External training	Win maximum investment benefits with minimum MES construction cost	1	4
External training	cybersec 2023 Taiwan Information Security Conference	2	24
External training	The 10th Manufacturing CIO Forum Kaohsiung	1	4
External training	Join hands to protect unlimited security and create a security protection circle for enterprises in Southern Taiwan Seminar	2	4
External training	Visitor registration management system manager training	3	2
External training	Taiwan Fuji THE ONE POWER YOUR WORK	1	4
Internal training	2023 Internal training-1	69	1
Internal training	2023 Internal training-2	7	1
Internal training	2023 Internal training-3	3	1
External training	iPAS Industrial Smart Transformation Promotion Class-Information Security and Industrial Application Trend Class	1	8

(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.