Resources Invested in Cybersecurity Management in 2025:

1. Cybersecurity awareness and training (4.5 hours total):
Information security and personal data protection awareness campaign (1 hour), email social media engineering drills and training (3 hours).
Information security awareness campaign + email etiquette (0.5 hours).

2. Conducted information security diagnostics and performed penetration tests on important servers, as well as server vulnerability and website security scans (initial and rescans), and made improvements and adjustments to high- and medium-risk items.

3. Updated firewall equipment at headquarters and Taichung and Kaohsiung branches, with replacement costs of approximately NT$600,000.

4. In accordance with the revised cybersecurity control guidelines for listed companies issued by the Financial Supervisory Commission, adjusted and implemented relevant cybersecurity measures, and continued to receive, transmit, and disseminate important cybersecurity intelligence.

5. Participation in cybersecurity-related training activities this year:

1.1 CTBERSEC 2025 Taiwan Cybersecurity Conference
1.2 2025/05/07 SP-ISAC Online "Introductory Cybersecurity Course - Information Risk Assessment and Risk Management" (3 hours)
1.3 2025/06/18 Cybersecurity Media - How to Build a Borderless Zero-Trust Ultimate Security Architecture in the Zero-Trust Era (3.5 hours)
1.4 2025/06 ISO27001-2022 Transition Course and Certification *1 person/16 hours; ISO27001-2022 Course and Certification 1 person/40 hours.
1.5 SSCP Cybersecurity Professional Certification Course (40 hours)
1.6 2025/10/30 SP-ISAC Hsinchu "Seeing is Believing: Building Evidence-Based Cybersecurity Defense Strategies Based on International Standards to Precisely Combat Internal and External Threats to Enterprises" Course (3 hours)

6. Conducted a fire drill in the headquarters data center in September; all functions were normal.

7. Adjusted the off-site backup mechanism and data backup for critical hosts, and conducted a disaster recovery drill in November to ensure data availability and integrity.
8. Added antivirus/EDR/MDR software in December to strengthen and complete the protection mechanism.

#The following items are scheduled to be presented at the board meeting in March, 2026.