Verification of Information Security Mechanisms & Cyberattack Management

When network attacks, malware, and other major information security incidents are detected, Cathay FHC and subsidiaries will initiate the Information Security Incident Reporting & Emergency Response Mechanism. Each company's information security emergency response team will respond to the incident in compliance with the "Major Information Security Incident Reporting & Emergency Response Management Guidelines for Cathay FHC & Subsidiaries." Cathay FHC will then compile material information security incidents (from all subsidiaries) for reporting to the Information Security Committee. In 2023, there were zero cases of material information security incidents.

Measures	Action Plans
Cyber-attack Drills	● Cathay Life, CUB, Cathay Century, Cathay Securities, and Cathay SITE commission experts as white hat hackers to conduct annual cyber-attack drills ● White hat hackers expose loopholes and scenarios, including connection status management, access control testing, and authorization escalation & bypass where IT systems are vulnerable to cyber-attacks by attempting to hack into the system
Information Security Assessments for Computer Systems	● Cathay FHC and subsidiaries commission thirty-party vendors to conduct information security assessments for computer systems, evaluating items such as information framework, network activity, vulnerability assessment, penetration testing, security settings, and compliance. The assessment allows us to monitor system safety, institute changes, and complete remediation for 100% of material risks identified from information security assessments
Threat Intelligence Sharing & Analysis Mechanism	● "Group Information & Threat Intelligence Sharing Mechanism" established to report and share material cyber threat intelligence for mitigation and protection ● Signed the "Memorandum of Understanding on National Cyber-security Protection & Intelligence Sharing" with the MOJ Investigation Bureau and "MOU to Jointly Combat Fraud & Safeguard Information Security" with the Criminal Investigation Bureau to strengthen the scope and depth of information security protection at Cathay FHC and establish a public-private information security cooperation framework to develop a cooperative protection mechanism

Information Security Implementation Results

	2021	2022	2023
Completion Rate for Information Security Training (%)	100	100	100
Total number of information security breaches	0	0	0
Total number of clients, customers and employees affected by the breaches	0	0	0

Note: Definition of information security breaches

1. Information security incidents that meet the standards of major unexpected events as specified in the "Procedures for Reporting the Scope of Major Unexpected Events by Financial Institutions and Other Compliance Matters."
2. Information security incidents that cause significant security risks to the company, result in business impact preventing normal operations, or cause substantial losses.
3. Information security incidents categorized as level 3 or above according to the internal regulations of the company.
4. Information security incidents leading to situations outlined in Article 4, Item 26 of the "Verification and Public Handling Procedures for Major Information of Listed Companies" by the Taiwan Stock Exchange Corporation.

Types: Intrusion and attack incidents, unauthorized operations by personnel, Distributed Denial of Service (DDoS) attacks, malicious software intrusion incidents, information security incidents requiring response due to media reports or requests from regulatory authorities.

Additional materials. Customer Privacy Protection & Response

Cathay FHC has dedicated sections on the official website for "Customer Data Protection Measures" and "Privacy Policies," where customers can learn about their rights and protections; a customer service consultation hotline to respond to for any inquiries or concerns regarding privacy policies or personal data usage; the "Cathay FHC Personal Data File Security Maintenance Plan and Personal Data Handling Procedures after Business Termination" to guide employees and vendors; and the "Data Subject Rights Management Measures" and channels for complaints and exercising their rights across the group to address the needs of customers and employees. In addition, Cathay FHC and its subsidiaries have established "Protocol for Responding to Personal Information Breaches" and processes for regular drills, requiring immediate reporting of personal data breaches to personal data management units. Interdepartmental "Emergency Response Teams" and reporting and handling processes are also established. Regular simulated training can strengthen the ability of employees to respond to personal data breaches, prevent impacts to the company, and reduce, as much as possible, damages to the affected individual. Cathay FHC also verifies the effectiveness of internal processes to identify deficiencies and perfect personal information protection measures. We had 14 data breaches events in 2023, in which 100% of data breaches events was involved with personally identifiable information. 61 customers were affected by such violation. Upon further investigation, Cathay FHC identified the case as personal negligence from financial advisors and sales agents in handling customer information. None of the cases were material data breaches or infringements on customer privacy. Cathay FHC has been able to settle the cases with customers and handled the situation accordingly. We will continue to organize employee training and strengthen awareness programs to ensure related employees fully recognize the importance of personal information protection. In addition, the group will continue to strengthen and monitor the use of customers' personal information and improve related protection measures to reduce future data breaches.

Personal Information (Data) Security Implementation Results

	2021	2022	2023
Personal Data protection training completion rate (%)	100	100	100
No. of personal data breach incidents (cases) Note 1	11	10	14 註 2
Personal data breaches to total information breaches (%) Note1	100	100	100
No. of customers affected by personal data breaches (customers) Note1	6,520	120	61
Percentage of customers who have agreed to the mutual use of their data among Cathay's subsidiaries (%) Note3	18	16	17
Note 1: Cathay started to disclose relevant data in 2021. It refers to incidents where personal data collected, processed, and utilized by Cathay Financial Holdings and its subsidiaries are leaked due to external intrusions (such as hacking, virus attacks, or theft) or human factors (negligence or intentional leaks,			

improper access, use, or loss).Data in "No. of information breach incidents," "Personal data breaches to total information breaches," and the "No. of customers affected by personal data breaches" include data for Cathay Life, CUB, Cathay Century, Cathay Securities, and Cathay SITE.
Note 2: All 14 cases in 2023 were investigations initiated by Cathay. For distribution details, please refer to Table 32 in the Appendix.
Note 3: The denominator for the calculation is the total number of customers after aggregation by subsidiary.