Sonix Technology Co., Ltd.

The Information Security Risk and Countermeasures

The information security risk management framework

The company has an "Information Security Team" led by the highest-ranking information unit executive, have dedicated information security supervisor and security personnel, responsible for information security management, planning, supervision and execution. The Team is mainly responsible for formulating and regularly reviewing information security policies, establishing incident reporting and response mechanisms, continuously improving defense capabilities, and enhancing employees' information security awareness. They reports to the board of directors regularly each year, the latest reporting date was 8th November 2024.

Information security policy

The company’s information security policy key points are as follows:

1. Refer to international information security standards and comply with domestic and foreign information security regulations, regularly revise the latest information security specifications.
2. Collaborate with external information security expert teams to detect and prevent security threats early.
3. Establish a multi-level defense structure and strengthen defense depth.
4. Strengthen information security professional capabilities and personnel, enhance internal information security planning and incident analysis and handling capabilities.
5. Continuously promote information security education and disaster recovery drills.

Information security management programs

The specific management plans that the company has adopted or implemented are as follows:

1. Next-generation firewall and intrusion detection system.
2. Endpoint antivirus and regular system vulnerability patching.
3. Multi-level antivirus and anti-hacking mechanisms for email and network, as well as joint defense systems.
4. Regular scanning and correction of website vulnerabilities.
5. Regular data backup and restoration mechanisms.
6. Regular information security awareness training and testing for colleagues.
7. Regular social engineering defense exercises.
8. Establishment of information security incident analysis, monitoring, and handling mechanisms.
9. Joining a security alliance to obtain the latest security information.
10. Weekly meetings to discuss information security risks and response measures

The company has strengthened its measures to respond to possible hacker intrusions, ransomware, and DDOS/APT attacks. We will continue to monitor external information security incidents, absorb new knowledge to strengthen information security controls, continuously establish multi-level protection and information security incident handling mechanisms, and strengthen the promotion of information security awareness to respond to the ever-changing network attack behaviors. In addition, when sensitive data needs to be delivered to vendors and customers, we always require the signing of a confidentiality agreement to regulate their confidentiality obligations.

Investments in resources for information security management

The resources the company has invested in information security management in 2024 are as follows:

1. Education and training: Complete all-employee education and training and questionnaires twice.
2. Social engineering drill: Conducted 4 email phishing drills to simulate attack scenarios and provide education and training to colleagues by clicking on phishing links.
3. The funding for [Information Security] related software and hardware exceeds NT$5 million.