Cyber Security Risk Management

- ## Cyber Security Risk Management Structure

  The Cyber Security Risk Management Structure of MediaTek Inc. ("MediaTek") is dominated by Cyber Security Committee ("Committee"). The Committee is composed of Cyber Security Incident Response Team ("CSIRT") and the supervisors of information technology department. The chairman of Committee is the chief information officer of information technology department. The Committee is accountable for managing, organizing, supervising and promoting execution of cyber security, such as planning and reviewing the policy of cyber security periodically, including reporting and emergency response of cyber security incidents, and reporting the result of cyber security safety check to Board of Directors periodically.

- ## Cyber Security Strategy

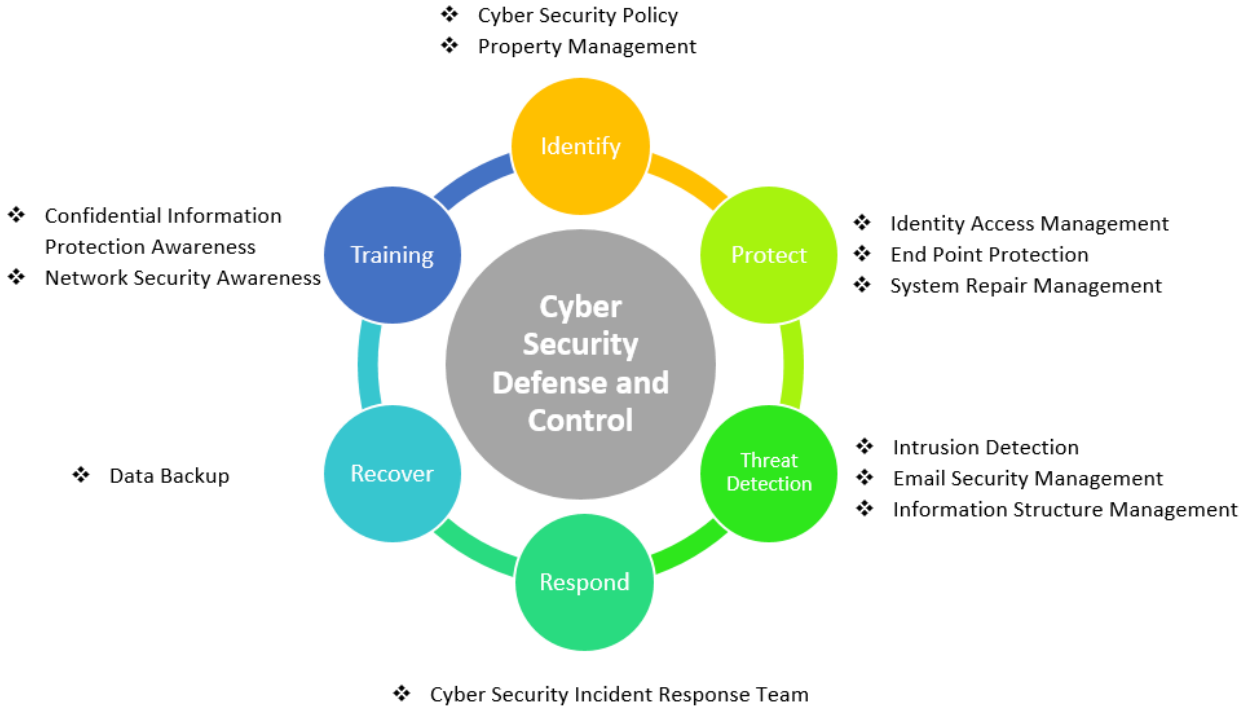
  1. To enhance cyber security management, MediaTek refers to international information security standards, including but not limited to National Institute of Standards and Technology Cybersecurity Framework ("NIST Cybersecurity Framework"), and complies with domestic and international cyber security laws and regulations to set cyber security rules.
  2. To ensure the confidentiality, integrity and availability of information, MediaTek adopts the strategy of "Multilevel Cyber Security Detection and Defense" to set up safeguards proactively before any cyber security incident happens and therefore to decrease the risk of any damage, unauthorized use or disclosure of information.
  3. To enhance the understanding and knowledge of MediaTek's personnel toward cyber security, MediaTek promotes the concept that "everyone shall be accountable for cyber security" through employee training programs.
  4. To minimize the potential damages resulted from cyber security incidents, Mediatek establishes CSIRT to take essential emergency action and resume normal operation within the shortest possible time. Upon occurrence of cyber security incidents, CSIRT will examine and investigate the incidents to provide the solution for improvement. The cyber security incidents shall be reported in accordance with MediaTek's rules of procedure.

- **Cyber Security Requirement for Suppliers**

  To enhance cyber security management toward suppliers of MediaTek, MediaTek requests all suppliers of MediaTek to comply with cyber security policy of MediaTek and sign necessary cyber security contracts and confidentiality agreements with MediaTek before cooperation.

- **Cyber Security Defense and Control**

  To enhance the cyber security management, MediaTek observes and examines cyber security circumstances of MediaTek and refers to NIST Cybersecurity Framework to formulate six items of Cyber Security Defense and Control measures.



  - **Identify**

    MediaTek develops risk management strategy that meets daily operations by inspecting environments, key sources and services, including formulating cyber security regulations and establishing the property management system.

  - **Protect**

    MediaTek formulates and implements defensive measures to ensure the key sources and services will not be affected by cyber security incidents, including Identity Access

Management (“IAM”), anti-virus software, end point protection and system repair management.

- **Threat Detection**
  MediaTek establishes the instant detection and warning mechanism for cyber security incidents, including email protection system, intrusion detection system, Security Operations Center (“SOC”) and periodically inspects the security of information structure.

- **Respond**
  MediaTek establishes CSIRT is accountable for cyber security incident emergency responses, such as incident investigation, review and proposing the solution for improvement. All cyber security incidents shall be reported and dealt with in accordance with MediaTek’s rules of procedure.
- **Recover**
  MediaTek sets up data recovery plan to be able to resume normal operation within the shortest possible time upon the occurrence of any cyber security incident.
- **Training**
  MediaTek promotes the concept that “everyone shall be accountable for cyber security” through employee orientation training programs, department education programs and Social Engineering Drill to enhance the understanding and knowledge of MediaTek’s personnel toward cyber security.