Risk from information security and cybersecurity failure, and threats to data privacy

Advancement in digital technologies has enabled service provider to launch new products and services with new business models to create or capture the business opportunities.

Through the 5G technology, the company over the next 5-10 years will be facing new challenges in developing/co-developing digital products and services with partners, and managing the complex future telecommunication network that is vastly different from today. The related emerging risks are the evolving complexity of technologies, and therefore the need to meet the increasing complexity and frequency of cybercrimes, as well as recruiting skilled workforce to develop and support future cybersecurity infrastructure and system. New technologies such as 5G will require new/revisited approaches to cybersecurity to ensure the company's resilience.

In addition, the company provides services to a large number of customers. It is essential to secure personal data properly in order to prevent the risk arising from the leakage of our customer's personal data. The company is also subject to comply with relevant laws and regulations including the Personal Data Protection Act (PDPA) and the General Data Protection Regulation (GDPR).

Impacts:

- Increasing risks of failure of company's cyber security measures due to the more sophisticated and frequent cybercrimes, may affect in the way we operate our business; for example, which type of data can be stored on cloud vs. our own premises, the investment required to operate and enhance security at our data centers. Failure to do so will incur financial loss and deteriorating trust from the customers.
- Gaps between existing and expected employee skills in cybersecurity may also result in slow progress towards business goals, financial loss and deteriorating trust from the customers.
- Growing requirements as specified by data privacy laws and regulations may impact the company's strategy, investment, and/or operation e.g. to enhance its data protection systems.

Mitigation Plans:

- Extend/expand security appliance tools to cover significant systems.
- Enhance information security and cybersecurity measures e.g. reviewing access control, maintaining a closed working environment and building IT security awareness across the company.
- Develop and enhance staff competencies related to cybersecurity.
- Apply suitable international standards and align with the Cybersecurity Act and Personal Data Protection Act, including (1) Set up Data Protection Office (DPO) to monitor and coordinate with other relating parties, to ensure that the company has proper processes with respect to the collect, use and disclose personal data. (2) Develop and implement data privacy policy and procedures in accordance with relevant laws and regulations, which are subject to a regular review.

Network and infrastructure disruption from increasing extreme weather conditions due to Climate Change

Telecommunications and information services are integral to the development of Thailand's digital economy and lifestyle. An uncontrollable disaster, natural disaster, or crisis event could potentially lead to the interruption of the Company's operating systems and business activities, posing widespread impact on consumers. With increasing trend of extreme weather due to climate change i.e. storm and flooding, our infrastructure may experience disruption more frequently if not managed properly.

Impacts:

- Business disruption; The failure of network can affect our business activities resulting in unachievement of business operational KPIs on network reliability.
- Company reputation; Frequent network failure can result in dropped customer satisfaction which affects customer's brand of choice in long-term
- Revenue loss; linking with customer satisfaction, frequent network disruption can affect company's delivery of services resulting in revenue loss and lower market share in long-term.
- Increasing maintenance cost; The damage caused by extreme weather events can increase maintenance cost and heighten capital expenditure in climate-proof infrastructures.
- Regulatory fines; network disruption can cause regulatory enforcement on company to compensate customers in an event of network failure.

Mitigation Plans

- AIS has set up redundancy for several key operating systems and infrastructure required to provide service as well as deployed automated monitoring system to ensure timely response and retain high service availability.
- AIS applies a Business Continuity Management (BCM) policy at both the corporate and functional levels and conducts an Annual Review and carries out exercises to practice and test the Business Continuity Plan, as well as having the Business Continuity Management System applied to certain critical services certified with ISO 22301:2019.
- The Company also adopted an infrastructure design that reduces the potential impact from disasters e.g. applying the EIA-222C standard to telecom towers to support higher wind speeds than in recorded Thai history, raising the height of base stations based on the level of heavy flooding in the year 2011.
- AIS conducts physical climate risk scenario analysis to identify high-risk operations and design local-specific mitigation plans to adapt with climate-related natural disasters