Annex A-3: Cyber Security

1 Brief Introduction

Annex A-3: Cyber Security is one of the foundational technologies of the digital transformation journey, without which, trust in the digital economy cannot be established and business would face difficulties in migrating to digital platforms. The Cyber Security industry will also need to constantly innovate to provide new solutions and services for companies in the new digital economy. The Cyber Security Technology Roadmap is developed to provide an overview of the cyber technologies of importance to the Singapore digital ecosystem.

2 Market Study

Global & Regional Trends

Five key global trends that have been shaping the global Cyber Security landscape are: increasing Cyber Security threat sophistication; erosion of the perimeter due to proliferation of IoT and mobile networks and cloud-based channels; diffusion of trust and identity due to the rise of multiple methods for users to access products and services and increased peer-to-peer transactions; proliferation of data at great velocities as organisations collect more data to generate insights and developments in and the increasing adoption of emerging technologies such as robotics, cognitive intelligence and quantum computing. The current global Cyber Security market is estimated to be US$100 billion in 2017 and to grow to US$173 billion in 2022 at a CAGR of 11.6%. The Asia Pacific Cyber Security market is expected to outperform the global market expanding from a US$20 billion market in 2017 to US$40 billion in 2022 at a CAGR of 14.6%.

Sectors such as Healthcare and Financial Services are likely to have the highest cost of data breach while Financial Services, information and communications technology (ICT), manufacturing, retail and professional are among the most highly targeted industries. The increasing reliance on technology and the Internet has resulted in citizens becoming exposed to the risk of becoming targets of cyberattacks. While Cyberattacks affect personal data and privacy of individuals, there is a significant loss of trust on organisations and Governments by the affected citizens and can lead to ramifications beyond privacy concerns and financial losses. Thus, many countries are taking measures to address this challenge.

Singaporean Trends

The Cyber Security market in Singapore was estimated at slightly less than half a billion USD in 2017 and is expected to grow to reach US$889 million in 2022 with a 15% CAGR. With 70% of market share, service-based Cyber Security market is expected to be the largest segment. By taking proactive steps across the various enablers, Singapore can accelerate its growth to be as high as 20%, growing its market to more than US$1.1 billion in 2022.Looking at the longer term, beyond 2022, Singapore's Cyber Security market growth will slow down as it enters a more mature stage. It is still expected to grow at 10% - 13% CAGR (from 2022 to 2030), achieving US$2.4 billion market size in 2030.

3 Technology Study

Contributions of Future Communications & IoT to Cloud Native Architecture

As a part of the overall technology roadmap recommendation, Singapore needs to establish a Cloud Native Architecture to improve access to emerging technologies amongst the stakeholders and enable the Services 4.0 ecosystem envisioned. Given how critical addressing security concerns of individuals and businesses for the adoption of several of these technologies, we believe that Cyber Security will play an important part in executing the Cloud Native Architecture as highlighted by the exhibit below. **Error! Reference source not found.** below shows in more detail how Cyber Security technologies will contribute to the Cloud Native Architecture.

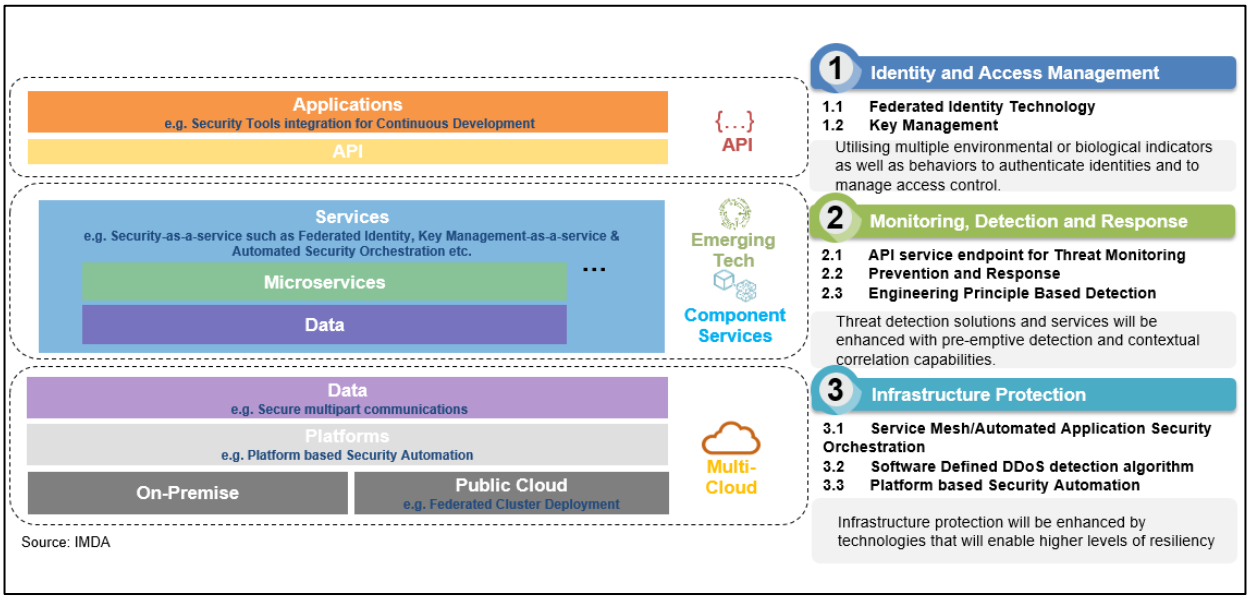

Exhibit 1: Contributions of Cyber Security to Cloud Native Architecture

4 SWOT Analysis

Our study of the Singaporean landscape and the global market for Cyber Security reveals specific strengths, weaknesses, opportunities and threats as discussed in the exhibit below. Cyber Security technologies will require a focused set of strategies, with Singapore's unique strengths and weaknesses in mind. These recommendations need to enable the development of local technology capabilities and drive adoption of Cyber Security technologies amongst industries to address key concerns, enable the development of related technology areas and to tap onto the strong regional growth potential. As a highly service-oriented country, Singapore already has active R&D efforts demonstrated by investments by industry and local research institutes, aiming to meet increasing demands from global and local Cyber Security players. Favourable Governmental regulation for Cyber Security is also expected to be a key enabler. Singapore needs to continue to provide a favourable environment with government support,

necessary regulatory and legal framework as well as develop the necessary Cyber Security talent and ecosystem which ultimately can help Singapore become a leader in Cyber Security.

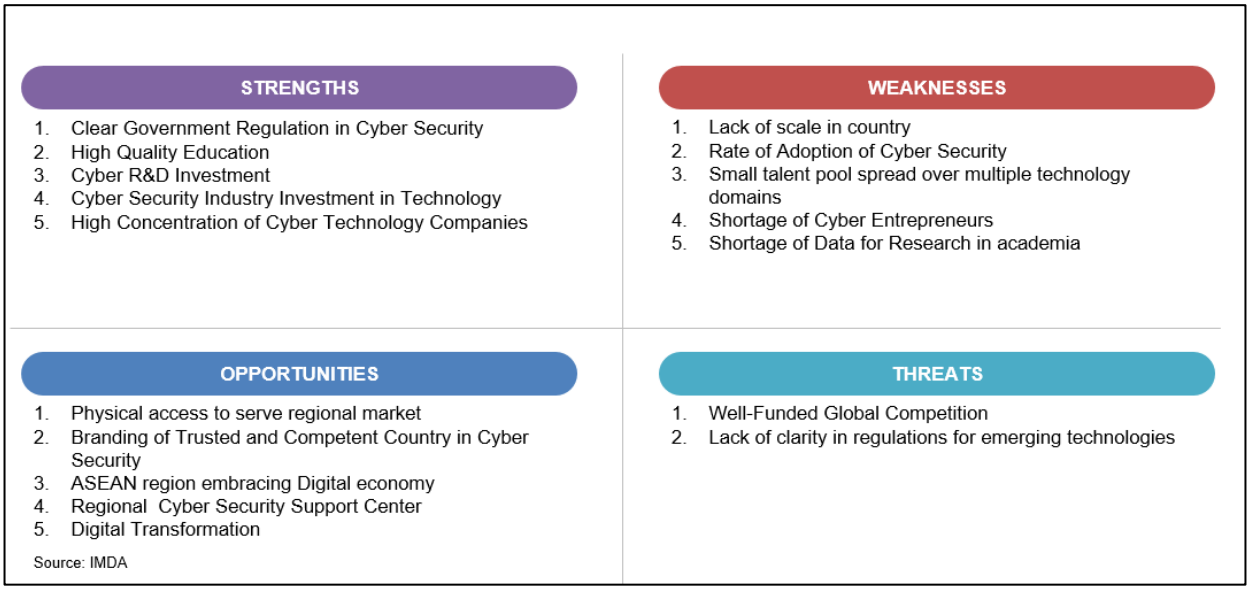

Exhibit 2: SWOT for Cyber Security

5 Recommendations

Based on the several guidelines developed from the SWOT analysis of Singapore Landscape, six main recommendations have been identified:

1. The Singapore Government should catalyse the availability of Cloud Native- Everything-as-a-service including cloud delivered Application Security and Identity and Access Management solutions, enable training on Cloud Security Orchestration and DevOps and establish a Cloud Services Marketplace.
2. The Singapore Government should invest in Privacy Engineering and Protection research and technologies, work with industry players to establish Digital Economy Tools such as consent platforms to encourage data sharing and establish platforms and technical tools that will help businesses meet data compliance requirements.
3. The Singapore Government should work with various stakeholders in the global ecosystem trying to set Cyber Security standards and framework for IoT, encourage efforts on commercialising IoT security products focussed on applications and specific priority sectors and work with industry stakeholders to encourage further adoption of eSIM.
4. The Singapore Government should take measures to enable Singapore to become a Cyber Security Hub for Emerging Technologies (Blockchain Cyber Security, Cyber Physical Systems Security and Quantum Technologies) such as developing relevant talent, enhancing research capabilities and encouraging industry collaboration.
5. The Singapore Government will need to take several measures towards building awareness, increasing adoption and developing an ecosystem such as encouraging Cyber Security entrepreneurs, developing technical talent and establishing critical Cyber Security Infrastructure.
6. The Singapore Government with a view to enable technology Commercialisation should encourage research Spin-offs, technology transfer for commercialising research and build a global Cyber Security community through enabling public-partner, multilateral and cross border partnerships.