ANNEXES A-3

CYBER SECURITY

CONTENTS

1 INTRODUCTION & OVERVIEW

The IMDA Cyber Security Technology Roadmap is a concerted effort to look into Cyber Security Technologies that are important for the Service and Digital Economy (SDE) to develop innovative solutions for the Cyber Security industry in Singapore and internationally. It takes into account innovations that would enable Singapore to move forward in our digital economy and to capture value in the provision of innovative Cyber Security technologies and services. It does not seek to cover all aspects of Cyber Security.

IMDA understands that the adoption and proliferation of Cyber Security in Singapore depends on multiple factors such as the Cyber Security ecosystem, regulation and talent development. The purpose of this Cyber Security roadmap is to consider how technology innovation in Cyber Security can advance the economic objectives of Singapore.

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 migrating to digital platforms. This would have a huge impact as these platforms are necessary for businesses to explore new opportunities and ensure that they continue to operate well in the age of digital disruption.

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 eco-system.

Over the years, the Singapore government has invested funding in Cyber Security research so as to encourage the translation of advances in research into suitable technology solutions. The Cyber Security Technology Roadmap takes into account the strength of the local Cyber Security research community that has been established through such funding.

In order to align and support the evolution trend of the ICM ecosystem, the Cyber Security Technology Roadmap is organised into the following domains to highlight the relevant cyber technologies:

a) Cyber Security (General)

b) Cloud Native Application

c) Internet-Of-Things

d) Cyber-Physical Systems

In each of these domains, we focus on technologies in the following categories:

a) Identify & Access Management

b) Assessment and Audit

c) Infrastructure Protection

d) Application Security

e) Monitoring, Detection and Response

f) Privacy Engineering

g) Investigative Technologies

h) Business Continuity & Disaster Recovery

This report also provides an update to the topic of security applications of Quantum Cryptography.

1.1 Cyber Security in the Digital Economy

Most businesses undergoing a digital transformation will need to be supported by suitable Cyber Security technologies. Businesses whose core services are not Cyber Security should make use of Commercial-Off-The-Shelf (COTS) products and services as the foundation of Cyber Security for their businesses.

As businesses in the digital age experiment with new ways to deliver services to their customers, Cyber Security solutions and services will also need to evolve and innovate to provide a continuum of cyber protection and enable trust in the new business delivery mechanism. In order to realise the addressable Cyber Security market, Cyber Security Service providers will need to find ways through the use of technology to reduce the friction of Cyber Security adoption by digital businesses. There is also a need for Singapore's Cyber Security Service providers to find their unique selling points in technology beyond the ability to purchase new speciality COTS software.

The Cyber Security Roadmap attempts to provide guidance to address the following areas:

a) How technology can increase the adoption of Cyber Security technology and services by businesses to ensure that businesses undergoing a digital transformation are operating in a cyber-safe manner?

b) How can Cyber Security businesses use innovation in Cyber Security technologies to increase revenue?

The Cyber Security Technology Roadmap will attempt to provide a vision of how innovations in the Cyber Security technology area can serve various sectorial clusters as they undergo their digital transformation.

The Cyber Security Technology Roadmap is intended to be a living document to be validated and updated periodically.

1.2 Cyber Security Technologies and services

As organisations recognise the value of Cyber Security investments, and the role of Cyber Security as an enabler of digital transformation, opportunities arise for the Cyber Security innovators. The various Cyber Security technologies and services offered can be categorised [1] as shown in Exhibit 1.

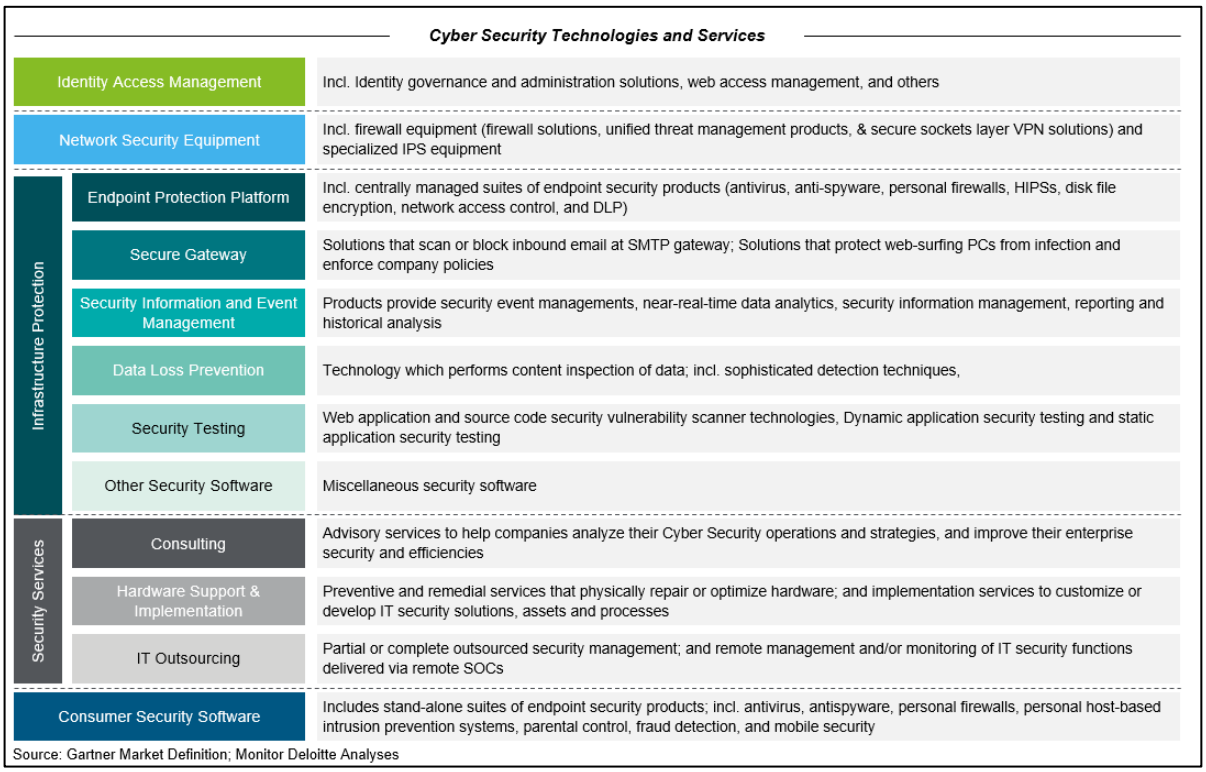

Exhibit 1: Taxonomy of Cyber Security Technologies and Services

2 MARKET STUDY OF CYBER SECURITY

2.1 Global Trends

In the World Economic Forum's 2018 Global Risk Report [2], cyber risk is recognised as one of the top commercial risks in both likelihood and impact. The exponential growth of digital technologies and innovation, along with ever increasing connectivity of devices and humans are creating endless opportunities for cyberattacks. Five key trends [3] [4] are reshaping the Cyber Security landscape globally:

Increasing Cyber Security threat sophistication

Criminals are increasingly engaged in cybercrimes as they realise cybercrimes offer high rewards with lower risk of consequences compared to traditional crimes. Attack tools continue to proliferate and achieve economies of scale through commercialisation, while the rise of cybercrime as a service has reduced barriers of entry.

Erosion of the perimeter

Innovations such as IoT, mobile, and cloud-based channels are dissolving the network perimeter, blurring the boundaries for protection. This trend will continue to be driven by

a) Companies striving to meet customers' expectations for products and services to be available 24/7 from any devices

b) Companies' increasing use of embedded sensors to collect data

c) Companies becoming integrated with vendors as they streamline back-end operations.

Diffusion of trust and identity

There are more ways than ever for customers and employees to access products and services. At the same time, blockchain and peer-to-peer networking has enabled anonymous transactions between individuals and businesses. This has made it challenging for organisations to manage digital identity and maintain trust within and between networks.

Proliferation of velocity and data

Improvements in technology have increased the accessibility of data. Organisations are collecting data at greater volumes, varieties and velocity to generate insights and make better decisions. This has increased the importance of data security to ensure customer privacy is protected.

Emerging technologies

Developments and increased adoption of emerging technologies such as robotics, cognitive intelligence and quantum computing create new cyber risks and complicate the Cyber Security landscape. However, they also create opportunities for enhanced Cyber Security solutions such as quantum encryption and AI-enabled cyber behaviour analytics. Cyber criminals and solution innovators will be in a race to exploit these emerging technologies.

While these Cyber Security trends are causing cybercrimes to become more frequent and costly globally, investments in Cyber Security lags. The disparate growth between the cost of cybercrime and Cyber Security signals a huge gap in enterprises' and users' ability to protect themselves against cybercrimes (Exhibit 2). Aside from being underprepared for a cyberattack, enterprises are forgoing digital transformation opportunities due to cyber risks. In Singapore, 52% of organisations have put off digital transformation efforts due to cyber risks [5].

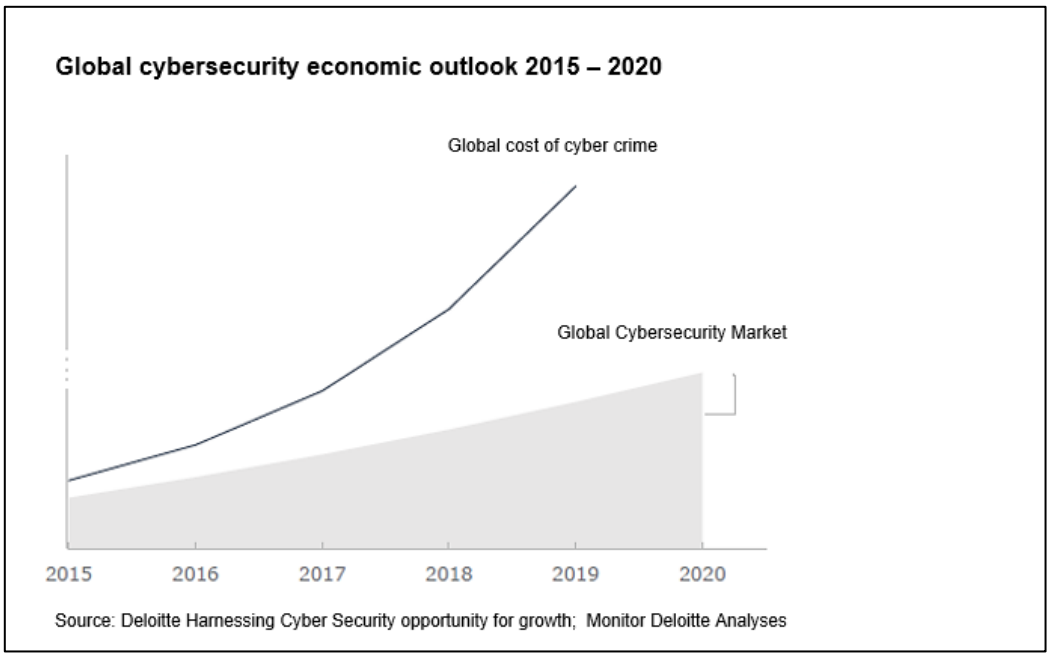

Exhibit 2: Global Cyber Security economic outlook 2015 – 2020 and Global and Regional Market Potential

2.2 Global & Regional Market Potential

The current global Cyber Security market is estimated to be US$100 billion in 2017. With a projected average compound annual growth rate (CAGR) of 11.6%, the market is predicted to achieve US$173 billion in 2022 [6] [7]. The Asia Pacific Cyber Security market is expected to outperform the global market at a 14.6% growth rate, expanding from a US$20 billion market in 2017 to US$40 billion in 2022 [6][7]. A detailed breakdown of the market is shown in Exhibit 3.

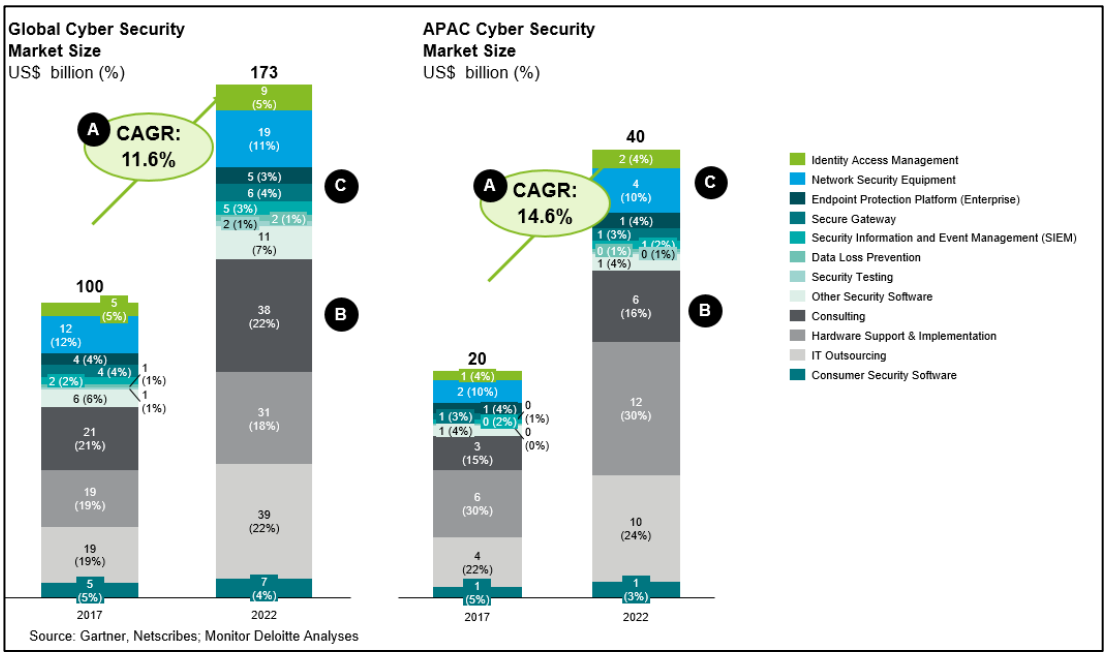

Exhibit 3: Global and APAC Cyber Security market size

2.3 Singapore Market Potential

Singapore's Cyber Security market is estimated at slightly less US$ 0.5 billion in 2017, but high growth is expected. At a predicted 15% CAGR, the Singapore market is estimated to double its market size to reach US$889 million in 2022 [3] [6] [8] [9] [10] [11] [12] as illustrated in Exhibit 4.With 70% of market share, service-based Cyber Security market is the largest segment, more so than in the global or APAC market.

Depending on the success of Singapore's efforts in developing the city as a Cyber Security hub, the pace of the Cyber Security market will vary. For example, Canada has taken concerted efforts to build Ontario into a Cyber Security hub by activating several ecosystem enablers. As a result, Canada has been able to accelerate Cyber Security growth in the region and Canada is now the world's 4th largest Cyber Security innovator as measured by VC deals [3]. Similarly, we believe that 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 (Exhibit 4).

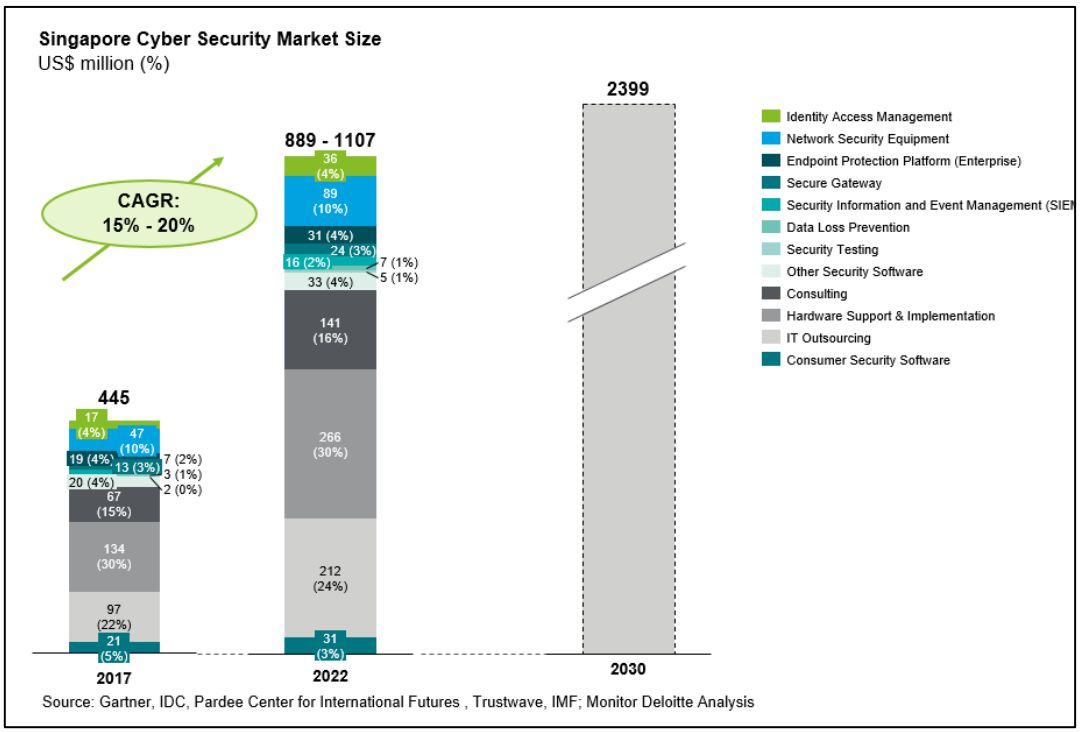

Exhibit 4: Singapore Cyber Security market size

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 a healthy 10% - 13% CAGR (from 2022 to 2030), achieving US$2.4 billion market size in 2030. This is on par with predictions for high-income countries, where Cyber Security spending is projected to be 0.4% of GDP [11].

2.4 Sector View

Certain sectors are more susceptible to cyber-attacks and we would expect enterprises in these sectors will be more likely to invest in Cyber Security. From a cost of data breach angle, these tend to be the heavily regulated sectors such as health care and financial services (Exhibit 5).

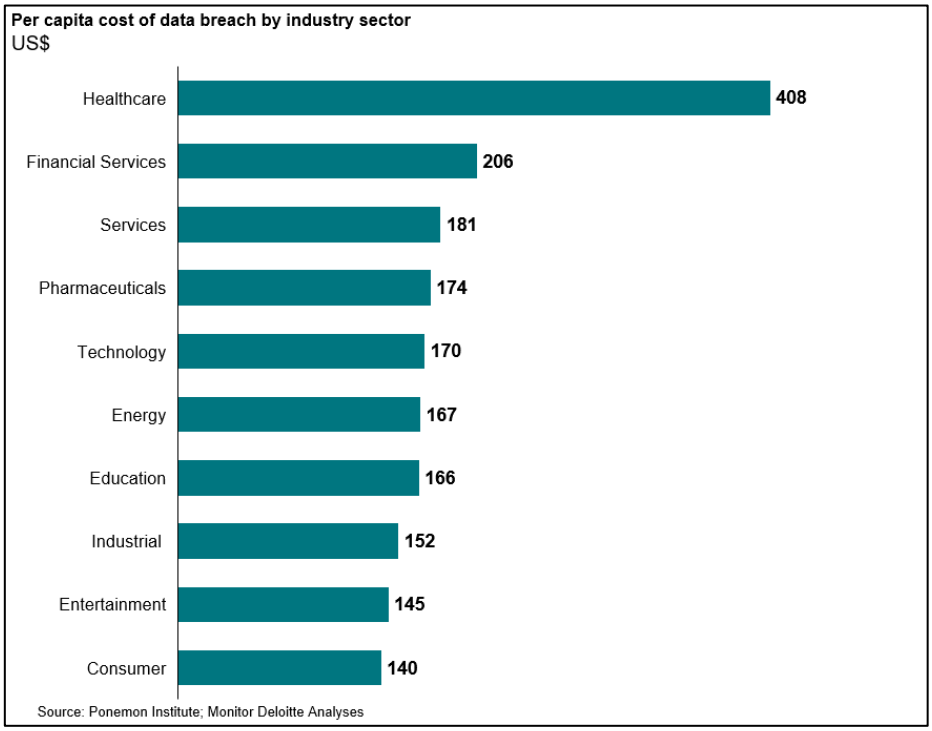

Exhibit 5: Top 10 industry sectors with highest data breach cost [13]

In fact, among the types of stolen personally identifiable information (PII), healthcare records fetched the highest premium. A healthcare record for a single individual was worth on average US$250 [14]. In comparison, payment card details for an individual cost on average US$5.40, while banking records cost US$4.12 each. This could incentivise attackers to focus on the healthcare sector when targeting PII data, which made up 10% of all data compromises in 2017.

While the cost of data breach in healthcare sector is high, it is less frequently targeted compared to other sectors. In 2017, the top five most frequently targeted industries based on security incidents are financial services, information and communications technology (ICT), manufacturing, retail and professional services [15] (Exhibit 6).

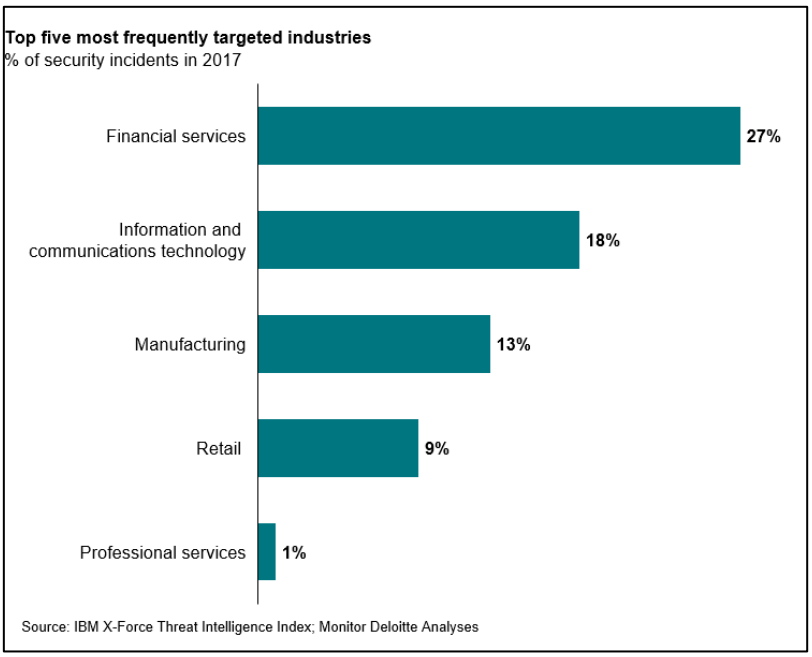

Exhibit 6: Top five most frequently targeted industries

Given the frequency and cost of attacks, it is no wonder that financial institutions spend three times more on IT security than non-financial organisations [16]. The Monetary Authority of Singapore (MAS) also plans to strengthen requirements on cyber resilience for Singapore's financial sector [17].

It is important to note that Singapore's Cyber Security Agency has identified eleven critical services sectors for which Cyber Security needs to be reviewed, which are aviation, healthcare, land transport, maritime, media, security and emergency, water, banking and finance, energy, infocomm, and the Government [18]. The Government's strategic focus on the eleven sectors will also influence the main sectors who will be large buyers of Cyber Security technologies.

2.5 Impact of Cyber Security to Citizens

The increasing reliance on technology and the Internet has resulted in citizens becoming increasingly exposed to the risk of becoming targets of cyberattacks. The dangers posed by different types of cybercrime have become very real threats. These threats come in a variety of forms and target networks, devices and users. The implications for individuals typically involve loss of personal data privacy and reputational damage, financial losses and increasingly, identity theft.

In 2017, 978 [19] million people in 20 countries were affected by cybercrime. Globally, consumers who were victims of cybercrime lost US$172 billion and each spent on average ~ 24 hours in resolving these cybercrime issues [19]. Globally, 6.5 percent of people were victims of identity fraud — resulting in fraudsters defrauding people of about US$16 billion [20]. The recent cyberattack on Facebook has resulted in the account of up to 50 million users being compromised [21]. Singapore has also experienced cybercrime. 1 in 2 Singaporeans surveyed were victims of cybercrime [19]. The recent attack on Sing Health has resulted in the records of 1.5 million Sing Health patients being compromised [22].

While Cyberattacks typically affect personal data and privacy of individuals, they do have broader implications on the political economic, and social systems that these individuals are part of. There is a significant loss of trust on organisations and Governments by the affected citizens and thus can lead to ramifications beyond privacy concerns and financial losses. Further, cyber-enabled crimes such as financial crime, crimes against children and fraud also pose distinct threats to society. As a result, many countries are taking significant measures to address this challenge.

For example, EU has passed the General Data Protection Regulation (GDPR) [23] that standardises data protection law across all 28 EU countries and imposes strict new rules on controlling and processing personally identifiable information (PII). This is expected to have significant implications on data protection for citizens. The UK has outlined several initiatives as part of its National Cyber Security Strategy [24] in 2016. One key initiative is "Building a More Secure Internet" that involves software and hardware "secure by default" to protect consumers. Another initiative focused on changing individuals and small business behaviour is the Cyber Aware campaign. This primarily involves the use of social media and partnerships to raise awareness to use stronger passwords and installing latest updates. The campaign also includes measures such as a hotline to report action fraud, "Take Five" campaign which is to help consumers protect themselves against financial fraud and guidance for consumer for smart devices in the home.

The Services 4.0 vision that has been laid out for Singapore will result in technology becoming more integrated into the lives of Singaporeans. Given the potential ramifications of cyberattacks on citizens and society, Cyber Security is thus a national imperative for Singapore and a critical part of the Technology roadmap.

3 TECHNOLOGY STUDY

3.1 Technology Adoption Readiness Map for Cyber Security in General

The technology adoption readiness map intends to inform the stakeholders on which technologies are expected to become mainstream in the coming years globally. A consistent time frame has been used in the narrative – now to 2 years (short-term), 3 to 5 years (mid-term) and beyond 5 years (long-term). Broadly,

- Technologies included in the now to 2 years timeframe are already or expected to be viable for adoption by the majority of industry players in now to 2 years (short-term);
- Technologies included in the 3 to 5 years timeframe have shown evidence of promising use cases, are being provided and afforded by a handful of companies but still not viable for mass adoption. These are expected to be viable in the next 3 to 5 years (mid-term);
- Technologies included in the beyond 5 years timeframe are mostly in the R&D stage and remain inaccessible to industry players. These are expected to become viable beyond 5 years (long-term).

The following table reflects the industry's view of the likely evolution and mainstream adoption of Cyber Security.

Categories	NOW - 2 YEARS	3 - 5 YEARS	> 5 YEARS
Identify & Access Management	Tokenisation, Continuous Behaviour Authentication	Scalable Attribute Based Encryption	Fine-grained authentication and access control
Assessment & Audit	Orchestration of Simulation	Breach and Attack Simulation	Human Agents Simulation
Infrastructure Protection	Deception Technology Physically Unclonable Function (PUF)	Security Orchestration and Automation Tools	Self-Shielding Dynamic Network Architecture
Application Security	Runtime Application Self-Protection (RASP)	Binary Analysis and Assessment	Automated Software Patching Tools
Monitoring, Detection & Response	AI/ML enabled Cyber Security	Threat Hunting	Fusion of Cyber threat Intelligence
Privacy Engineering	Secure multi-part Communications	Privacy-Preserving	Privacy-Preserving

		Technologies (1)	Technologies (2)
Investigative Technologies	Cyber Forensics – Blockchain, Multimedia, Video	Cyber Forensics – Vehicular, Infotainment, Drone	Cyber Forensics - Robotics, Autonomous Systems, Certification Testing Tools
Business Continuity	Integrated Orchestration of heterogeneous network	Resource Efficient Continuous Data Protection (CDP)	Blockchain in Disaster Recovery

Table 1: Technology Adoption Readiness Map for Cyber Security

3.1.1 Now to 2 Years

3.1.1.1 Tokenisation

Tokenisation is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token, which has no extrinsic or exploitable meaning or value. It acts as a reference (i.e. identifier) that maps back to the sensitive data through a tokenisation system. The mapping from original data to token uses methods which render tokens infeasible to reverse in the absence of the tokenisation system, for example using tokens created from random numbers. It is also this feature that makes it difficult for an organisation to conduct data mining activities associated with token use. Research in data analysis methods when token use is in place would greatly enhance the usefulness of tokenisation.

3.1.1.2 Continuous Behaviour Authentication

This area of technology focuses on the use of biometric or sensor signals that would be typical of a person interacting with the devices or their environment as a means to provide in-line authentication thereby improving the security posture from the “one-time” authentication which has deficiencies in certain use cases.

The technology may use (but are not limited to) a combination of signals as described in the following:

a) Typing behaviour

b) Breathing/Heartrate

c) Focus of Eyes/Pupils

d) Proximity to environmental sensors

3.1.1.3 Orchestration of Simulation

There are currently many commercially available solutions and services that would allow for simulations of enterprise networks for the purpose of Cyber Security testing. The challenge faced today is the ability to orchestrate an enterprise’s network in a very quick manner and with enough fidelity to

achieve realism in simulation, such that exercises and experimentations would reflect the exact response and function of a high fidelity digital twin.

3.1.1.4 Deception Technology

Deception technology is a means to provide early and accurate detection by laying a minefield of attractive decoy systems and content to trip up attackers. The aim is to have automated capabilities in detection, analysis and defences against zero-day and advanced attack warnings in real time. Deception technology enables a more proactive security posture by seeking to deceive the attackers, detect them and then defeat them, allowing the enterprise to return to normal operations.

Deception technology aims to lure attackers to attack the 'decoy' assets which are simulated to have the look and feel of a real asset. In allowing the adversary to attack the decoy or deception environment, the adversary or malicious insiders essentially reveal themselves to the organisation thereby giving early warning to the organisation.

An example of an open source community effort would be the "Honey Pot Project" from OWASP. This project develops the honeypot software that participants can place in their networks to enable collection of data that would be shared collectively by the community to maximise intelligence from the cyber-battlefield that exists between attackers with criminal intent.

3.1.1.5 Physically Unclonable Function

A Physical Unclonable Function (PUF) is a physical entity that is embodied in a physical structure that serves as a unique identifier for semiconductor devices. Due to the inability to control the exact microstructure of physical factors introduced during manufacture of each device (and its components) and its mathematical unclonability, it renders a PUF truly unclonable. Due to these properties, PUFs can be used as a unique and untamperable device identifier. PUFs can also be used for secure key generation and storage as well as for a source of randomness. There are proposed standards specifying the security requirements and the test and evaluation methods for PUFs, signifying industry interest in this area.

This is an important area of technology as its applicability is in the ability to create unique identity for the devices for the purpose of asset identification. The PUFs are also important in cryptography for its ability to provide the randomness required for secure key generation. We can see proposed technologies in this space looking to make use of quantum processes on materials to provide the PUF.

Within Singapore, there are existing research in NUS that is attempting to map PUFs of power generators to use them as unique IDs in a distributed power grid. There is still work on the design of identification/authentication protocols (PUF-based security protocols) leveraging PUF that would be required to complement existing work.

3.1.1.6 Runtime Application Self-Protection (RASP)

RASP is a technology that improves the security of software by monitoring its inputs and blocking those that could allow attacks. It is triggered when an application runs to protect the runtime environment from unwanted change and tampering runs on a server. It is designed to detect attacks on an application in real time within the context of the environment. By using RASP to continuously monitor the app's behaviour, attacks can be identified and mitigated immediately without human intervention.

3.1.1.7 Machine Learning (ML) / Artificial Intelligence (AI) enabled Cyber Security

Machine Learning and Artificial Intelligence is also highly applicable to Cyber Security. Singapore shows potential in and has made investments into research in the following areas:

a) Behavioural Tracking methodologies/algorithms to reduce false positives

b) Intelligence of vulnerabilities and attacks detection

c) Monitoring, detection and response

d) Contextual awareness and correlation in threat identification

e) Fast scaling technology to keep up with fast evolving baseline

AI is expected to be particularly valuable in supporting detection of cyber intrusion or attacks through its capability to respond and analyse incidents. The response can manifest itself as defensive moves such as manoeuvring defences to meet/close off the vector of attack, reducing the attacked areas and automatic isolation of affected areas. This would limit the impact of possible attacks and reduce the need for human intervention.

There is also a need to develop automated cyber data analysis that can result in lower false positives (and false negatives) that can alleviate the workload of first level operators. This will help reduce the need for first level operators and can free up staff to perform higher level work, which contribute to staff retention and career development.

Algorithms for detection and analytics technology will need to be further developed to become fast scaling as the analysis required for behaviour characteristics will increase beyond those of end users, to include manufacturer-to-manufacturer (M2M) as IoT and Virtual/Augmented Reality applications are introduced in service sectors.

The technologies developed in this area finds a wide range of use cases. From being able to provide insider detection to being able to customise the level of cyber mitigation for end users (e.g. the level of mitigation required for digital natives versus new entrants to technology). The same technology can also be applied to high throughput networks such as Telco infrastructures.

These technologies would be particularly interesting to Security Operations Centres (SOCs), Managed Security Service (MSS) providers and application developers who will be able to use the advances of these technology to better enable their business models.

The Singapore government has invested in this area of research in the local universities such as NUS, SUTD and NTU. Technology companies are encouraged to seek out collaborations with these research units to translate these research outcomes to commercially viable products.

3.1.1.8 Secure Multi-Party Communications (MPC)

This technology allows multiple parties to jointly compute a function over their inputs while keeping each individual party's input private.

Secure Multi-party Computation has wide applications in privacy preserving fields in decision making, such as voting computation, statistics computation and securing databases.

NTU has been working actively in the area of MPC, using mathematical tools from algebra, combinatorics and lattices, and have made significant theoretical progress on various aspects of efficient MPC constructions.

3.1.1.9 Forensics – Blockchain, Multimedia, Video

Blockchain Forensics

As blockchain technology finds application beyond the crypto-currency circles, tools for forensic investigation of blockchain applications will need to be developed to aid in blockchain implementation. Tools developed must be able to investigate whether manipulation of the blockchain through known

weaknesses in the system has taken place. With such audit and forensics tools available, there would be increased confidence in the use of blockchain to achieve its purposes.

Cyber technology solutions providers who could package such technology into an integrated tool would be interested in the development of this technology. End users of such technology will include blockchain based businesses that are looking to increase trust in their stakeholders.

Multimedia Forensics

Under the digital economy, multimedia tools will be used extensively in the provision of digital services. The protection of intellectual properties of multimedia content is vital to content providers as any tampering of digital licensing and fingerprinting for the purpose of piracy will result in loss of revenue.

In addition, multimedia may also have additional use in the area of identity management. Thus, specialised tools in multimedia forensics will need to be developed to analyse evidence in the event of piracy and identity theft.

Specific areas to be developed include forensics capability to investigate circumventing cryptographic access control, secure delivery, and finger-printing of multimedia content and discovery of the source/time of leakage.

Where multimedia (e.g. object liveliness factors) is used as a supporting tool for identity or authentication, forensics tools will need to be able to investigate whether tampering had occurred.

Content developers/companies will be most interested in this area of technology development as this would protect their content from piracy which would ultimately mean protection of revenue. Technology companies using multimedia as an auxiliary to their main service will also need to ensure that the multimedia aspects are not their weakest link.

Video Forensics

In a digital society/smart city, there will be an increased in use of cameras to help achieve secure and seamless service delivery. Across areas as diverse as food outlets, financial institutions and traffic monitoring, data points collected would be useful in incident investigation. Advances in video manipulation technology complicates matters as false video evidences can also be generated. To counter this, tools specialised in video forensics need to be developed so that accurate “raw” evidence can be analysed and presented as evidence in the court of law.

The tools to be developed would need to accurately and reliably

a) Determine that the video has not been manipulated

b) Determine that the video is a raw recording (as compared to a AI generated recording)

c) Pick up items of interest using video analytics capabilities

Law enforcement agencies and security consultancy firms providing forensics investigation services are parties that would be interested in this area of technology development.

3.1.1.10 Integrated Orchestration of Heterogeneous Network

Increasingly, businesses are being built on a combination of on premise and cloud infrastructure. This results in significant challenges when it comes to disaster recovery as these infrastructures are managed differently. The current approach to this operational gap is to orchestrate the networks separately. Technology solutions that will allow integrated orchestration of heterogeneous networks would improve the level of disaster recovery capabilities of the organisation.

The National R&D Cyber Security Laboratory funded by NRF should enable this area of research as it has the potential to translate into new capabilities in disaster recovery solutions.

3.1.2 3 to 5 Years

3.1.2.1 Attribute-based Access Control

Attribute-based Access Control (ABAC) is an approach to managing access whereby access rights are granted to users through the use of policies that combine attributes together. The policies can use any type of attribute such as user, resource, object, environment attributes, etc.

This authorisation model provides dynamic, context-aware and risk-intelligent access control to resources as access control policies can include specific attributes from many different information sources to define permission sets to resource and data. In doing so, organisations can achieve efficient regulatory compliance and allow enterprises flexibility in their implementations based on their existing infrastructures.

Organisations would benefit from the implementation of ABACs as it provides a finer grain of control over resources and data as personnel move across job roles over time. There are research outcomes funded by the Singapore Government in SMU's Secure Mobile Center over the last 3 years that can be explored for translation. Interested parties should approach SMU Secure Mobile Center for discussions on the commercialisation of the technology. The focus in 3 to 5 years' time would be to find ways to make this technique scalable.

3.1.2.2 Attribute Based Encryption in Context Based Access Control

Attribute based encryption as applied in Context-based Access Control (CBAC) is often a feature of the firewall software, which intelligently filters TCP and UDP packets based on application layer protocol session information. It can enhance CBAC based technology appliances to support data confidentiality. Hence, enabling fine grained access control of the data traffic with more expressive policies.

3.1.2.3 Breach and Attack Simulation

Breach and Attack Simulation technology is a means to conduct continuous automatic security testing. This is especially important in a highly complex security eco-system and an ever-changing IT environment, where the deployment of new systems and security solutions is becoming more time consuming and costly. Ongoing automatic testing enables organisations to not only confirm whether existing Cyber Security measures are always working, it also makes it possible to boost their security posture by highlighting the pathways of penetration an attacker could use to reach their critical assets. The tool can be used to highlight gaps in security postures and thus help prioritise investment in Cyber Security.

3.1.2.4 Security Orchestrations and Automation Tools (SOAR)

SOAR is an integration of orchestration processes, automation, incident management and collaboration, visualisation and reporting under a single interface to enable security operations centre (SoC) to more accurately process large volumes of data produced by Cyber Security systems and help identify and remediate attacks which may be imminent or underway.

SOAR technologies enable organisations to collect and aggregate vast amounts of security data and alerts from a wide range of sources. These assist human and machine-led analyses, as well as the

standardisation and automation of threat detection and remediation with the aim to help improve their security operations proficiency, efficacy, and quality, and manage cyber incident efficiently.

The traditional SOAR vendors are dependent on simple workflows to execute response actions. While these workflows work well for out-of-the-box threats, they fail in an organisational context and require fine tuning during deployment and the cost of maintenance of these workflows increase the barrier of adoption. While most organisations believe that SOAR as a technology could lower threat response time considerably, they do not believe that the current SOAR solutions are manageable. An innovative approach to updating response workflows with relevant actions continuously that lowers the maintainability and exhaustive set of automated responses to different types of attacks across architectures is the need that would provide better outcomes.

The use of SOAR could also attempt to negate the effects of employee turnover that might affect the fluctuation of level of expertise within the security teams at different time periods. SOAR can also be used for the purpose of threat hunting.

3.1.2.5 Binary Analysis and Assessment

Binary analysis refers to a program testing process where human analysts and/or automated systems scrutinise the underlying code in software to discover, exploit and defend against malice and vulnerabilities, oftentimes without access to source code.

There is a need for such techniques as Commercial-Of-The-Shelf (COTS) software will seldom enable access to source code to test for security vulnerability. Currently, there are already binary analysis tools and services. But the field of binary analysis is continuously being improved to reduce the possibilities of false positives or false negatives.

The Singapore Government has invested in this area of research in our Autonomous Universities and have achieved good research outcomes that have been tested at competitions worldwide. It is a good time to translate such research to commercial offerings that would continue to provide an enhanced level of security for products that we would be using in the digital society.

Binary analysis tools will need to be continuously improved. In the 3 to 5 years' time frame, research outcome in the following areas are expected to be mature and ready for translation:

a) Binary Analysis against malware attacks

b) Dynamic taint analysis techniques

c) Real Time application security analysers

d) Hybrid analysis mapping techniques

e) New isolation primitives to reduce system complexity

An additional specialised area of focus would be the vulnerability detection in mobile applications. Notable funded research outcomes in this area that would interest technology partners would reside in NUS and NTU.

Software security solutions testing providers would be interested in this technology capabilities to be integrated into their solution suite. In addition, these technologies can also be used to create secure software testing services that can be used to certify software having reached a certain level of security. Such technologies are also captured in Singapore Universities such as NUS and NTU through Singapore Government funded research.

3.1.2.6 Threat Hunting

The premise behind threat hunting is that we are operating in a zero-trust environment where threats are already inside the network waiting for the perfect moment to initiate an attack. This is especially true as it is now difficult to enforce a true perimeter with the usage of mobile and IoT devices. Today, threat hunting is still heavily dependent on human analysis to make the connection. Automated threat hunting that is able to sense from the integration of data from different Cyber Security SIEM, tools and threat intelligence platforms would enable enhanced capabilities that does not exist currently.

Some of the advance features of such solutions would include:

a) Deep and vast presence in multiple cyber-threat arenas allows detection of the threat as they take shape and identification of the threat actor before they intrude the organisations' network.

b) Designated Indicators of Compromise (IOCs) provide analysts with the "right" and most up-to-date indicators. Taking into consideration the implementation of any indicators is simply not enough for providing ongoing high-levels of security, it is vital to provide IOCs that are most relevant to the organisation's context.

c) Intelligence-driven threat hunting capabilities that enable analysis of malware and deep understanding of the profiles of different threat actors based on ongoing research. In addition to raising alerts regarding the threat, it is necessary to provide the entire background story, incorporating recommendations for mitigation, etc.

3.1.2.7 Privacy Preserving Technologies (1)

With more applications and services going Cloud Native, a corresponding privacy preserving regulatory framework and technology suite is required to:

a) Mask & publish personal identifiable data to protect confidentiality & privacy while enabling data sharing and aggregation.

b) Enable joint computation and collaborative mining on masked data.

c) Govern information access and data protection as well as detect abuse and access violations.

The purpose of privacy preserving technologies are to protect personal data and ensure the users of technology that their information can remain confidential and that organisation has a technical means to undertake data protection.

The technologies should minimise personal data collected and used by service providers and merchants, use pseudonyms or anonymous data credentials to provide anonymity, and strive to achieve informed consent about giving personal data to online service providers and merchants.

The technology should provide the possibility to remotely audit the enforcement of agreed conditions with a service provider. The technology when implemented correctly has the potential to increase digital services in smart cities projects and commercial services.

Privacy Respecting anomaly detection technologies

This area of technologies deals with how anomaly detection can be done in a manner that would still respect privacy. Today's technology used in the Enterprise requires that the data passing through anomaly detection engines to be in the clear. Increasingly, there is an expectation that employees would demand certain privacy such that current methods where organisation typically requires all employees to submit their permission for access to employee generated data to be in the clear for inspection may not work.

Technologies in this area would include anomaly detection using Homomorphic encryption techniques and Random Multi-party Perturbation.

The key challenge in this area is the ability for these techniques to be able to be applied to complex real world scenarios and their ability to scale in implementation without affecting accuracy.

Searchable Encryption

Searchable encryption (SE) was invented to provide data privacy, and at the same time offer a limited way of accessing the cipher text without decryption.

NTU has research projects in private queries on encrypted databases using fully homomorphic encryption. They have investigated fundamental types of queries, such as conjunctive, disjunctive, and threshold queries, as well as advanced queries, such as wildcard (IEEE TDSE 2017, 2018), Design of public key encryption with equality test. We studied constructions of public key encryption with equality test, which can be applied to searchable encryption such as keyword searchable encryption (TCS 2018, Inf. Sci2016, Comp J. 2016, ACISP 2018).

Homomorphic Encryption

Fully homomorphic encryption (FHE) is an encryption scheme supporting computations of arbitrary functions on encrypted data without decryption. FHE is one of the most promising cryptographic tools for protecting sensitive data stored in databases. This area of research is still very nascent. We may see some applications in very specific use cases in a 3 to 5 years' timeframe but generic applicability of homomorphic encryption would be an area where the community expect to take beyond a 5 years' timeframe to mature.

The current state of homomorphic encryption allows for simple functions such as Boolean queries (AND, OR), simple keyword searches.

3.1.2.8 Cyber Forensics – Vehicular, Infotainment, Drone

Vehicular and Infotainment systems forensics

As vehicles become more connected and autonomous, more data and telematics can be collected from their usage. The data generated and collected through connected infotainment systems in vehicles can be pieced together to find out what happens in the event of an incident. Hence, there is a Cyber Security need to develop forensics tools that facilitates investigation. These tools will need to take into account different vendors' data structure. To better facilitate investigations, they should be able to understand and re-trace interactions between vehicular systems and connected infotainment systems.

Law enforcement agencies and security consultancy firms providing forensics investigation services can potentially be the parties who will be interested in this area of technology development. Same goes for automotive companies as they would need to be able to conduct related independent investigations to meet automotive regulatory requirements.

Drone Forensics

Drones will be increasingly used to provide services in the digital economy, from postal delivery, multimedia production, and surveillance to F&B services. Embedded within these drones are a host of technology ranging from global positioning systems, cameras, proximity radars, operations systems and applications.

Drone forensics can be important in several scenarios, particularly so when a drone goes rogue due to hostile takeover or when drones are the "witness" (incidental collection of environmental data) of particular incidents. There are very disparate tools at this point in time to collect each type of data but lawful admission of such data would still be difficult. Certified tools that can perform forensically sound aggregated collection of these data within drones would need to be developed.

Law enforcement agencies and security consultancy firms providing forensics investigation services may be the parties that would be interested in this area of technology development.

3.1.2.9 Resource Efficient Continuous Data Protection (CDP)

Continuous data protection (CDP) refers to the automatic real-time backup of incremental changes to data. This allows for data restoration to any point in time. CDP-based solutions can provide fine granularities of restorable objects ranging from crash-consistent images to logical objects such as files, mail boxes, messages, and database files and logs

The challenge with CDP is that they are resource-intensive and they create additional workload on the network and the server. Improved efficiency in the methods for capturing the continuous changes would enable CDP technologies to be used more extensively.

3.1.3 Beyond 5 years

3.1.3.1 Fine-grained Authentication and Access Control

Authentication and access control has become mainstream and is available in products. The advances in this area would be in how technology can provide granular access control with ease. Most innovations in this area rely on how access control can be further tightened by authorised personnel to lower organisational risk further. Such technology can utilise multiple data points available such as environmental, biological indicators, known behaviour or context of events to provide the level of access to required resources.

Authentication and access control product developers would be interested in this area of technological development to improve their product offerings.

3.1.3.2 Human Agent Simulation

Cyber Security testbeds technologies are important aspects of research that can produce real-world-implementable capabilities. A particular field of research that is being developed are test agents that mimic human behaviour with respect to Cyber Security related actions. Such research provides data points to test cyber technologies in the absence of real world test subjects.

This technology would be interesting to cyber developer companies who can use them to test their own products in development. The technology is also applicable to end-user companies who can use it to validate/evaluate new products and test their organisations' cyber posture.

3.1.3.3 Self-Shielding Dynamic Network Architecture Moving Target Defence (data, endpoint, network)

The current static nature of computer networks allows attackers to gather intelligence, perform planning, and then execute attacks at will. This situation creates a low barrier of entry and puts any given computer network at risk. The research into the area of Self Shielding Dynamic Network Architecture would look at how the use of virtual machines can enable quick changing defensive/mitigation mechanism can be employed to deter mapping of static network configurations which can be exploited to conduct safe extraction of data once internal machines are compromised.

3.1.3.4 Auto Software Patching Tools

The ability to create the software patches that can address the susceptibility found from vulnerability analysis will greatly improve software security. Auto software patch creation has been funded as a

research topic by the Singapore Government and it has been getting good results for software with a reasonable (line of) code base.

The research challenge for the longer term is to transform the current software into a more complex software (above 2 million lines of codes). Associated with this development, additional validation tools should also be developed to certify the feasibility of such tools. For instance, validation tools need to identify if software patches cause other downstream problems when they are created. Tools that simplify the process of testing patches prior to application into operations environment will need to be developed.

Software security solutions testing providers would be interested in this technology capabilities to be integrated into their solution suite. In addition, these technologies can also be used to create secure software testing services that can be used to certify software that have reached a certain level of security. Such technologies are captured in Singapore Universities such as NUS and NTU through Singapore Government's funded research.

3.1.3.5 Fusion of Cyber Threat Intelligence

Cyber threat intelligence today still requires the human operator to do the sense-making across disparate intelligence gathering sources based on the experience of the operator. Research of how unstructured intelligence data can be integrated into coherent sense-making in the domain of Cyber Security will greatly improve security operations centre functions. Taking it a step further, the ability to sense-make across cyber intelligence data and non-cyber related events would create additional unique capabilities.

3.1.3.6 Privacy-Preserving Technologies (2)

Privacy-preserving outsourced computation of encrypted data

Increasingly, there is a demand for outsourcing a private function computation through public data without privacy leakage to unauthorised parties. It should include the ability for encrypted data belonging to multiple users to be processed without compromising on the security of the individual user's (original) data and the final computed results.

This is an area of research that needs to be conducted by focusing on the key outcome of scalability and translatability into real-world systems.

Attribute-based keyword search over encrypted data

Verifiable Attribute based keyword search (VABKS) is an area of research where a cryptographic solution allows a data owner to selectively allow access to specific keyword searched over the encrypted data. This would be increasingly important as business applications are deployed to the cloud and data encryption takes place to protect user data. Without a means to conduct data analytics over encrypted data, it becomes an impediment for a business to further improve upon the services they can provide to the end users or to improve upon their business models.

There is already existing research that has been conducted in this area. The remaining question is in their scalability and practicality of implementation. As this is reasonably complex, there is still a question of the viability of translation and commercialisation. Question to ask would probably include what is the level of performance against homomorphic encryption today?

Enterprise organisation would benefit from the commercialisation of this technology once the technology has overcome the complexity in implementation which would include the organisation understanding how this the technology works and being able to assigned the correct attributes to each object. In 3 to 5 years' time, the focus is on scalability of the technology.

3.1.3.7 Cyber Forensic – Robotics, Autonomous Systems, Certification Testing Tools

Robotics / Autonomous Systems forensics

As robotics and other autonomous systems for smart city implementation and manufacturing become popular, there is a need to develop tools and techniques to enable investigation when cyber incidents affect such systems. Of particular concern would be DDoS attacks or alteration or functions through cyberattacks on such system that can potentially halt services and affect citizen's quality of life in a smart city.

Forensics technology to be developed will need to be able to predict attack paths and source of attacks in the event accountability needs to be established for legal reasons.

Law enforcement agencies and security consultancy firms providing forensics investigation services would be the parties that would be interested in this area of technology development.

Cyber Forensics certification testing tools

As we progress in the development of forensics tools, there will be a need to have these forensics tools tested such that the results from these tools can withstand scrutiny. Test methodology and technology for verification of these forensics tools will need to be developed such that the confidence in the use of these tools would be high. The intent will be to increase the capability of forensics tool developers to improve their toolset.

Forensics tools developer will be interested in this area of technology development.

3.1.3.8 Blockchain in Disaster Recovery

It is natural to think that blockchain will negate the need for database backups and change the premise of disaster recovery. This is because blockchain writes all data onto the distributed ledger which essentially backs up data automatically across the distributed ledger. However, the challenge today is in its performance. Writing a record onto the blockchain and gaining consensus across the distributed ledger is still a slow process as compared to traditional databases we have today. Research into consensus algorithms that would be able to match the efficiency of current database record-writing speed would improve the adoption of blockchain in the field of high data resiliency systems.

3.2 Technology Adoption Readiness Map for Cloud Native Application

Categories	NOW - 2 YEARS	3 - 5 YEARS	> 5 YEARS
Identify & Access Management	Federated Identity Technology	Key Management	
Assessment & Audit	Cyber Security Ratings services	Cloud security testing and assessment tools	
Infrastructure Protection	Service Mesh/Automated Application Security Orchestration	Software Define DDoS detection algorithm	Platform based Security Automation
Application Security	Container Security Technologies	Security Tools integration for Continuous Development	Security Tools integration for regulatory compliance
Monitoring, Detection & Response	AI Service endpoint for Threat Monitoring , Prevention and Response	Engineering Principle Based Detection	Chaos Engineering
Investigative Technologies		Continuous monitoring and support for investigation	
Business Continuity	Recovery by Snapshots Recovery by Redeployment	Federated Cluster Deployment	

Table 2: Technology Adoption Readiness Map for Cloud Native Application

This chapter calls out specific Cyber Security technologies of importance that is specific to Native Cloud Applications in the respective areas.

3.2.1 Now to 2 Years

3.2.1.1 Federated Identity Technology

Federated Identity Technology enables users to access a network of different services through just one data identification portal. This allows timely support and access of different identity management systems, even across different applications. For instance, when two domains are federated, the user can authenticate to one domain and then access resources in the other domain without having to perform a separate login process.

Technologies used in Federated Identity include SAML (Security Assertion Mark-up Language), OAuth, OpenID, Security Tokens (Simple Web Tokens, JSON Web Tokens, and SAML assertions), Web Service Specifications, and Windows Identity Foundation.

3.2.1.2 Cyber Security Ratings Services

These services provide continuous and independent quantitative security analysis and scoring for organisation entities. They measure the level of security implementation and threat exposure that an organisation is exposed to. Subsequently, they provide remedies to increase the security posture of cyber exposure areas.

Service Mesh / Automated application security Orchestration

Microservices architecture become more complex as the number of microservices use to put together a service increases. A service mesh is a network of microservices that allows user to interact with many applications at the same time. As a service mesh grows in size and complexity, it can become harder to understand and manage. Solving this issue requires substantial effort in discovery, load balancing, failure recovery, metrics, and monitoring. A service mesh also often has more complex operational requirements like A/B testing, canary releases, rate limiting, access control, and end-to-end authentication.

Service Mesh security capabilities provides the underlying secure communication channel, and manages authentication, authorisation, and encryption of service communication at scale. With appropriate implementation of service mesh, service communications can be secured by default, allowing application owners to enforce policies consistently across diverse protocols and runtimes – all with little to no application changes. Examples of service meshes includes Istio and Linkerd.

3.2.1.3 Container Security Technologies

Commercial applications depend more and more on microservices. Container technologies are increasingly used to deploy these microservices due to its fast deployment and resiliency. Containers are now such integral elements of software delivery that enterprises are demanding security in and around containers.

There are needs to translate current research and methodologies in evaluating container security into commercial products.

These technologies should address the following:

a) How containers can be assembled and updated securely?

b) How security controls are put in place (and if they are functioning correctly)?

c) How the OS is hardened?

d) How services are segregated?

Improvement to the techniques and tools in this area will greatly improve the security assurance of applications and services meant to be deployed using container services. Smaller start-ups may be interested to develop tools and services to serve this market.

3.2.1.4 API Service Endpoint for Threat Monitoring, Prevention and Response

Service monitoring technology to ensure service uptime is already available in current Cloud Native Deployment. New services will need to be created to enable existing threat monitoring, prevent and response technology to be extended to the microservices endpoint architecture.

3.2.1.5 Recovery by Snapshots /Recovery by Redeployment

The simplest form of application recovery for Cloud Native applications would be in the use of recovery from snapshots. Snapshots are instances of an application residing on the cloud resource that can set to be backed up periodically. Most Cloud Service Providers (CSP) provide this as a tool within the cloud admin panels.

Recovery by Redeployment is the newer approach to recovery by the redeployment of a workload in a very rapid fashion, often fully orchestrated with minimal to no downtime. This method is made possible with cloud orchestration technology such as Kubernetes and requires a mature deployment and support pipeline.

3.2.2 3 to 5 Years

3.2.2.1 Key Management

The advances made in Hardware Security Modules (HSM) allow for placement of key management at the edge of the companies' cloud deployment. By providing for Key Management activities closer to the data, users and asset validation functions can be greatly improved. Key Management as a Service allows the digital business to be agile by shifting the key management costs to a usage based cost (instead of incurring capital cost in purchasing the Key Management solutions). Besides, it is easy to maintain across multiple cloud service providers.

3.2.2.2 Cloud Security Testing and Assessment Tools Cloud

The cloud is increasing being used as the mainstream infrastructure for deployment of digital services. Techniques and tools are required to be developed to address the unique security concerns relating to the use of the cloud infrastructure due to its massive scale and dynamic configuration possibilities. The increased complexity that the data can also reside in multiple jurisdictions further complicates security/privacy testing requirements.

Such testing tools should include the following considerations:

a) Multi-layer testing

b) SLA based testing

c) Large scale simulation

d) Hypervisor security

e) Data remnants

f) On demand provisioning of resources

g) Serverless implementation

h) Application security including application APIs & information access abuse testing

Cloud infrastructure and Cloud security audit service providers would be interested in this area of technology development.

3.2.2.3 Software Define DDoS Detection Algorithm

The deployment of Software Defined Networks introduces the ability to detect and react to DDos attacks in the data plane. But it also introduces the possibility that the control plane itself can be attacked and be brought down, thereby creating a DDos.

The technological algorithm in this area needs to be lightweight and use the data from the control plane to detect possible attacks and react accordingly.

This area of technology exploration and translation should lead to how SDNs should be securely deployed and be able to discover mitigation measures and techniques to prevent the SDN environment itself from being a victim of DDos attacks.

3.2.2.4 Security Tools integration for Continuous Development

Integration of tools into the DevOps Process to achieve DevSecOps.

Collaboration from development security team and operations team is required to develop such tools that allow greater efficiency and productivity. This philosophy involves building automated security into applications so it's baked-in rather than applied after the fact.

If applications are built by development teams with security in mind, Ops can deploy them faster and with the peace of mind knowing that Dev understands how important reliability and security are.

A way to tackle the abovementioned problems is to integrate security testing into the CI/CD process. The security tests must integrate seamlessly into the current development environment, such that the software engineers do not have to leave their accustomed environment. Continuous Security goes in line with usable security such that developers can focus on their main tasks without ignoring security issues.

3.2.2.5 Engineering Principle Based Detection

Cloud Native Applications are microservices-centric, portable, and automatically managed. Security tools used in detection methods in a Cloud Native system must:

a) Be tooled to handle Cloud Native components like containers, serverless, and microservices. At the same time, they must work seamlessly with detection technology designed for virtual machines, physical servers, and traditional networks.

b) Effectively reduce and normalise security alerts: Because Cloud Native workloads can be ephemeral, alert volumes may be higher than that of a traditional system and can easily overwhelm even the most sophisticated modern detection infrastructure.

c) Be in Cloud Native environment because of the sheer scale and velocity of such systems. A bulk of the alerts covered by the detectors are either discarded or acted upon without being specifically reviewed through a critical scaling factor.

Modern detection engineering requires the adoption of engineering principles to security analysis. In a Cloud Native system, this practice becomes existentially critical — without it, security detection will be untenable.

Security investigation for Cloud Native workloads can be complex because of all the distributed components and API services, so monitoring and security investigation must minimise the impact to

performance and demand for storage. This necessitates a monitoring/investigation architecture that is distributed, lacks system bottlenecks, and can scale with the workloads.

3.2.2.6 Federated Cluster Deployment

Cluster Federation allows for orchestration of a clustered application to be spread across multiple clusters across geographical locations. These technology application enables owners to connect disparate clusters running in different environments. For example, a large enterprise running Kubernetes as an orchestration layer can federate an on-premises cluster with Cloud Service Provider's Kubernetes implementation running in the public cloud. Operators and DevOps engineers can manage these federated clusters in the same way they handle regular clusters. Federated clusters can go a long way in delivering the promise of multi-cloud and ensure business continuity.

3.2.3 Beyond 5 years

3.2.3.1 Platform based Security Automation

Platform based Security Automation attempts to automate and orchestrate security operations to enable efficiency in a cyber-analyst's workflow. Such platforms serve as a layer to connect multiple (Cyber Security) point products by acting as the connective tissue to integrate the dozens of discrete point products to automate and orchestrate complex workflows that execute in seconds instead of hours or more if performed manually.

3.2.3.2 Security Tools Integration for Regulatory Compliance

Research needs to be conducted to look at the integration of security tools into the DevOps development process to enable integration of automated policy enforcements of regulatory standards, security workflow and corporate security standards without specialised training required of the systems developers and operations integrators.

3.2.3.3 Chaos Engineering

Chaos engineering is the process of testing a distributed computing system to ensure that the system can withstand unexpected disruptions in its functions. It is so named because it relies on concepts from chaos theory, which focuses on random and unpredictable behaviour. The goal of chaos engineering is to continuously conduct controlled experiments that introduce random and unpredictable behaviours in order to discover weaknesses in a system.

In a microservices architecture, any function may involve many software components stitched together at runtime. From a security monitoring and detection standpoint, this means detection logic and controls cannot rely on a prior understanding of the operational state and security health. Rather, Cloud Native security must embrace chaos engineering principles – experiment proactively, test often, and remediate fast.

3.3 Technology Adoption Readiness Map for Internet-of-Things

Categories	NOW - 2 YEARS	3 - 5 YEARS	> 5 YEARS
Identify & Access Management	Biometrics, Certificates and Lightweight Key Management, eSIM		Integration of authentication protocols
Assessment & Audit	Security Testing and vulnerability Analysis	IoT framework assessment tools	Cyber validation tools for regulatory assessment for sector specific domains
Infrastructure Protection	IoT Honeypots Microsegmentation	5G Security Tools for auto-patching of vulnerable embedded systems	Next Generation IoT Infrastructure protection
Application Security	Lightweight DTLS chips	Source and Binary code application protection for IoT Devices	Modelling and Analysis of Wireless Sensor Networks
Monitoring, Detection & Response	Real time monitoring for continuous threat detection and management	Dynamic detection, profiling, and accounting of IoT connections	Emerging threats research specific to IoT architectures
Privacy Engineering	Secure aggregation or fusion of sensor data for privacy	Edge computing data security	Personal gateway
Investigative Technologies	IoT Memory Forensics		Tools to support IoT forensic framework

Table 3: Technology Adoption Readiness Map for IoT

This chapter calls out specific Cyber Security technologies of importance that is specific to Internet-of-Things in the respective areas.

3.3.1 Now to 2 Years

3.3.1.1 Biometrics, Certificates and Lightweight Key Management

The definition of Internet-Of-Things (IoT) is very broad and could mean multiple things to different people. For the purpose of the cyber roadmap, it looks to provide insights for (1) Consumer Devices and (2) Sensor Devices.

For consumer devices, biometrics and its derivatives of implementation (such as continuous authentication) are technologies to look out for in this timeframe. These would include facial recognition, voice recognition, gesture dynamics and handling dynamics in additional to fingerprint scan.

For IoT sensors, users should look at certificate based solutions and where possible lightweight key exchange mechanism to allow for ease of updating.

The current consensus is that IoT solutions today are presented to the end user and systems integrators as a package and does not allow for individual (modular) implementation of security controls on the devices.

3.3.1.2 Security Testing and Vulnerability Analysis

Many IoT devices, especially sensors, are made for specific purposes and have limited capabilities to update current firmware once deployed. It would be important that security testing and vulnerability analysis are conducted on the devices before full-scale deployments. Technologies developed in binary level code analysis (static and dynamic) and smart fuzzing technology will enable a higher degree on security assurance prior to development.

3.3.1.3 IoT Honeypots

IoT honeypots are a form of deception technology that is deployed as bait systems for systems that are integrated with IoT systems, especially where the IoT devices are fitted with systems that may difficult to update due to the nature of embedded hardware.

IoT honeypots provides several purposes. They provide early warning systems akin to a “canary in the coal mine” when an attacker tries to penetrate an organisation’s systems via its IoT implementation.

Secondly, IoT honeypots allow for the organisation to understand the weaknesses of their IoT implementation in a safe but realistic manner by studying how a real world cyber attacker would try to compromise their system and adjust their implementation accordingly.

The challenge with IoT honeypots is the ability to simulate the fidelity of the IoT devices to be exactly like the actual IoT device and the placement of the IoT honeypot to channel the attackers to it instead of the actual system.

3.3.1.4 Microsegmentation

Microsegmentation is the ability to create secure zones in data centres and cloud deployments that would isolate workloads from one another and secure them individually. It is aimed at making network security more granular.

While traditional segregation by firewalls separates zones by network segments, microsegmentation gives greater control over the growing amount of lateral communication that occurs between servers

or workloads, bypassing perimeter-focused security tools and limits the potential for lateral exploration of the deployed network.

This technology is available now but additional research can be done to enhance the efficiency of microsegmentation technology in the long term.

3.3.1.5 Lightweight DTLS Chips

Datagram Transport Layer Security (DTLS) are sometimes included as part of IoT devices to protect end-to-end communication among IoT devices as IoT devices suffer from resource constraint and are unable to run the fully featured IP stack. These devices' security functions such as Random Number Generators (RNG) can be exposed to the application layers to generate random numbers for the purpose of encryption functions.

3.3.1.6 eSIM

Increasingly, we note the use of eSIM or embedded identification over physical SIM in IoT devices. eSIM is a form factor of certificate for device identification with a connectivity enabler.

The provisioning mechanism is an important factor that would determine the level of security it can provide. The ability to be compatible with international telco networks is important and moreover, for security and economic reasons, a domestic standard is critical for the national deployment and management of IOT security.

There are already ongoing eSIM standardisation efforts that have started currently and we may begin to see companies and organisations building systems or infra around and using eSIM in the now to 2 years timeframe with the expectation of this taking of strongly in the 3 to 5 years timeframe.

3.3.1.7 Real time Monitoring for Continuous Threat Detection and Management

The Internet-of-things (IoT) technologies are expected to be a dominant technology in use in the move towards a smart city and digital society. Connecting many IoT systems provides the "smarts" that power our smart economy and digital services.

Due to the unique characteristics of IoT devices which can be low powered and fitted with a limited capacity CPU, specific protocols in communications and higher layer stacks have been developed to address the resource constrains. The protocol behaviour could deviate from your standard networking stack. This customisation addresses the usability aspect of IoT but also introduces many security challenges.

One of the promising areas of research that would augment existing monitoring tools would be in the in-line vulnerability discovery of IoT specific protocols implementation.

It is expected that cyber technology providers would be interested in the development and translation of such technology. They will in turn provide these capabilities as either products or services that they can provide to IoT products or solutions providers.

3.3.1.8 Secure Aggregation or Fusion of Sensor Data, for Privacy

To adhere to data governance and regulation, this technology looks at how the aggregation of sensor data can enhance the state of privacy required. Individual sensor data could possibly disclose a particular sensor's status, thus fusion of multiple sensor data could not only enhance the privacy, but also provide a concise data summary aggregating a number of sensor data. The ability to provide relevant data while maintaining privacy would enhance AI modelling.

An example of such technologies would be PATE, Private aggregation of Teacher Ensembling that will defend against stealing model parameters and training data.

3.3.2 3 to 5 Years

3.3.2.1 IoT Framework Assessment Tools

IoT Security frameworks are actively being developed by the IoT ecosystem. These frameworks ensure that developers do not overlook security in the development of their IoT solutions due to lack of knowledge in IoT security considerations.

This frees developers and architects to focus on features and capabilities without burdening their development efforts with security considerations. As these frameworks come into adoption, assessment tools will be needed to simplify the assessment process. These should include vulnerability assessment of common commercially available IoT architectures.

There are multiple work-in-progress in the Internet Engineering Task Force (IETF). For example, in the domains of Authorisation and Authentication in Constrained Environments(ACE), Constrained Restful Environment (CoRE) and CBOR Object Signing & Encryption (COSE) amongst others. These works can be further adapted to include the security controls that can be further supplemented.

It is expected that IoT security companies would be interested in the development in this technology area. They can incorporate such technologies into their product to be sold to IoT developer companies. They could also offer assessment services to end-user to validate that the required service levels are met.

3.3.2.2 5G Security

There are current efforts to look at 5G security with efforts towards 3GPP standardisation, such as topics on 5G security architecture for enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (uRLLC) and massive Machine Type communications (MTC). Manufacturers will be shipping 5G products in one or two years' time, conforming to the 3GPP 5G standard but adoption will take place over a long 3 to 5 years' timeframe.

3.3.2.3 Tools for Automated Patching of Vulnerable Embedded Systems

This would be the continuation from the technological inroads been made to detect vulnerabilities in embedded systems to have tools that would be able to automate the creation and testing of these created patches. Tools should be able to create the required compiled patch and to create a link that would enable the patch to intercept during run-time instead of the original embedded vulnerable firmware.

Embedded technology providers would be interested in this technology as addressing the vulnerabilities of an embedded system is currently very lacking. The ability to build trust in this area will enable better market adoption of systems with embedded technologies.

3.3.2.4 Source and Binary Code Application Protection for IoT Devices

Source and binary code protection for IoT devices application would be needed for devices to be protected against unwanted reverse engineering. Technical means to do so includes the use of encrypted strings in programming, scrambling address lines through additional logic or replacement of library functions. Effective code protection techniques may require substantial investments in expertise to implement. Technologies that would be able to abstract and automate these techniques would enhance the ability for code protection without the high cost associated with it.

3.3.2.5 Technology for Dynamic Detection, Profiling & Accounting of IoT Connections

The importance of being able to dynamically detect, profile and identify legitimate IoT devices on the network holds an important fundamental of IoT security in operations.

The challenge today is in the ability to efficiently do this with minimal effort of administrators having to manually register the huge number of devices that may come onto the network in a very ad-hoc manner. The technology will need to be able to identify legitimate IoT devices vs malicious or compromised devices put in place by the adversary.

The technology can be embedded as a module in gateway equipment that would be able to see all inbound and outbound network traffic and have the computing cycles required to be able to identify specific devices without foreknowledge of their existence.

The technology will benefit both Industrial and Consumer gateways in IoT solutioning.

3.3.2.6 Edge Computing Data Security

Edge computing is based on the concept where the IoT sensors would generate a vast amount of data which is needed to be analysed closer to the origins of the data (aka Edge of the network) for quick decision making and response. It would not be efficient to transport the data to a remote centralised data centre due to the low bandwidth and latency involved.

This also means that data residing on edge devices, which could have limited processing power, will need to be adequately protected. This introduces numerous challenges with respect to data security and privacy. Many use cases can be shown to indicate that sensitive data will be collected as part of the process. For example, Personal Identification Data (PID) can be collected by location sensors as part of the provisioning of location based smart services. There is also a need for edge devices to share data amongst themselves to create the analytical outcome required.

“Security by Design” would hold the best promise of ensuring data security of these edge devices but realistically, this is often seen as an exception rather than a rule for the devices that we can get commercially. Research would be required to find the best ways in which we would be able to ensure data security at the edge.

3.3.2.7 IoT Memory Forensics

Most IoT devices are designed with limited storage memory and most activities happen in the volatile memory space. The threat of firmware based malware has limited mechanisms for detection and analysis.

IoT volatile memory forensics can be a possible way to provide for a mechanism to detect the presence of modified firmware, through ROM shadowing. The advances in this area of work seeks to use the volatile memory acquisition as a means to collect evidence pertaining to firmware-based rootkits or malware.

3.3.3 Beyond 5 years

3.3.3.1 Integration of Authentication Protocols

Federated Identity technology (e.g. OAuth, OpenID) allows for the use of a single identity to be used to sign on to several services. An extension to this would be the development of integrated authentication IoT protocols like MQTT which could leverage existing identification to access and control deployed IoT devices. For example, the use of smartphone serving as authenticating for other

personal devices like smart watch by way of delegated authentication will be one of the many possible integrations. These would be useful in use cases such as smart home, smart building and smart city.

3.3.3.2 Cyber Validation Tools for Regulatory Assessment for Sector Specific IoT Domains

As we transit to a digital economy with different sectors and industry transforming themselves digitally, it would soon be realised that different sector will be required to meet different level of Cyber Security due to the nature of the industry/sector. Tools specific to the assessment of these industry will need to be developed to enable implication of assessment need.

Sector regulators will be interested in this area of technology development.

3.3.3.3 Next Generation IoT Infrastructure Protection

We are already seeing international groups working on potential roadmap for the next-generation (communications) infrastructure. The focus of such roadmaps is to provide for higher speed/throughput and highly reliable networks integrated with security concern. The expectations are that the next generation of wireless connectivity will provide speeds of 1 to 100 Gbps to the end user and MU-MIMO capability of 100 to 1,000 simultaneous independently modulated beams effectively providing speeds in the tens of terabytes per second.

Apart from providing precision localisation to a fraction of an inch, supplementing GPS, 6G imaging techniques will identify any person or moving object. This intelligent, immersive infrastructure will support low-latency virtual reality (VR), augmented reality (AR), and seamless telepresence. The implications to Cyber Security to support such features would be an area of research that needs to be conducted.

3.3.3.4 Modelling and Analysis of Wireless Sensor Networks (WSN)

Wireless sensor networks are networks in which thousands of sensor networks are deployed. Each of these sensor nodes can be small in size with limited memory space and processing power. In many cases, the nodes can also be constrained in the ability to accessing power. This constricts the security mechanism that can be implemented on such sensors. There is a need to research into abstraction techniques for design space exploration and verification of non-functional properties through modelling and analysis such that the security related issues with WSN can be studied and addressed to better design secure WSNs.

3.3.3.5 Emerging Threats Research Specific to IoT Architectures

Threat Research on IoT architectures: IoT ecosystems are inherently complex. Today there is a lot of focus on the end device, but the ecosystem contains multiple components such as platforms, databases, connectivity, APIs, mobile interfaces, etc. Our experience is that it is not that these individual components are insecure, but it is at the interface of two or more such components that the greatest vulnerabilities lie. The need to research multiple IoT architectures and their associated vulnerabilities and the emerging threats that exploit these vulnerabilities is key to building Secure IoT Deployment Capabilities. With this in mind two specific areas of research is being proposed:

a) Vulnerability assessment of common commercially available IoT architectures: It is important to assess these commercial available architectures to ascertain the attack surface and impact of the attacks

b) Discovering emerging threats specific to IoT/ICS architectures: Run a honeypot of "rooted" IoT devices that represent different architectures (this may include physical and virtual devices) to ascertain the velocity and veracity of new threats

Data from such a setup can be used to discover zero days by further mining the vulnerabilities and threats for known Indicators of Compromise.

3.3.3.6 Personal Gateways

The concept of personal gateway as a technology for use in data privacy and filtering for interesting permutations of how data sharing and privacy can be achieved. Personal gateways can allow for a consent model to be implemented easily as the control of data sharing is held by the individual. The aggregation of personal gateways into communities can also introduce anonymity into the data such that specific data cannot be tied back to the individual during analysis.

3.3.3.7 Tools to Support IoT Forensic Framework

IoT deployment is expected to be pervasive in the digital economy. There is an increase interest in how digital forensics techniques can be used to conduct digital forensic investigations in IoT-based infrastructures.

Up to this point, IoT has not fully adapted to digital forensics techniques owing to the fact that the current digital forensics tools and procedures are not able to meet the heterogeneity and distributed nature of the IoT infrastructures. Gathering, examining and analysing potential evidence from IoT environments when they are to be used as admissible evidence in a court of law when a cyber-incident happens poses a challenge to digital forensics investigators and Law Enforcement Agencies (LEA).

Frameworks for IoT Forensics investigation are expected to be developed over the next several years and the supporting forensics tools to enable the implementation of the IoT Forensics framework will need to be developed to enable the ease of operations.

When cyber incidents happen for IoT deployment, they need to be looked at from a deployment level instead of just at the device level. A framework for investigation is expected to be developed in the next few years for this purpose. Tools to enable implementation such an IoT Forensics framework will need to be developed to enable ease of operations and to facilitate effective forensics investigation for IoT infrastructure.

Law enforcement agencies and security consultancy firms providing forensics investigation services would be the parties that would be interested in this area of technology development.

3.4 Technology Adoption Readiness Map for Cyber-physical-systems

Categories	NOW - 2 YEARS	3 - 5 YEARS	> 5 YEARS
Identify & Access Management	Trusted Computing Based Identity Protection	Access management framework to all components in CPS	
Assessment & Audit	Digital Twin	Software & Framework Extension to Digital Twin	Model-based security testing for cyber-physical systems
Infrastructure Protection	Data Diodes	Deception based Protection	Layered Defence
Application Security			Techniques for auto-patching of CPS vulnerability
Monitoring, Detection & Response	Real time monitoring & threat detection in CPS	Automation in vulnerability detection and incident response in CPS	Protocol-oblivious anomaly detection in CPS
Privacy Engineering		Data Protection and Security of Training Data	Lightweight and resilient crypto for Cyber-Physical Systems

Table 4: Technology Adoption Readiness Map for Cyber-Physical-Systems

This chapter calls out specific Cyber Security technologies of importance that is specific to Cyber Physical Systems in the respective areas. It is noted that this is a particularly niche area and that technologies specific to this space in still nascent.

3.4.1 Now to 2 Years

3.4.1.1 Trusted Computing Based Identity Protection

A series of trusted computing technologies are being reapplied into protecting endpoints in critical infrastructure, including TCG DICE, Cambridge CHERI, ARM trust zone/PA, Intel SGX. These are being applied into smartphone chips as well as IoT chips, for stronger hardware/software protection.

The high number of breaches and the sophistication involved are driving OEMs to incorporate security at the design phase of the device. Part of Identity management consists of the authentication of identity,

meaning that one needs to provide secret information for verifying a claimed identity. For storing and computing with the secret information (e.g. a private key), one has to store and compute the secret securely, whereas a trusted execution environment (e.g., DICE, SGX, TrustZone, etc.) is needed.

At the hardware level, this establishes TPMs (trusted platform modules), which integrate cryptographic keys in the chips that can be used by the software layer for device authentication. However, the keys involved may still be vulnerable if they are shared on a bus. This issue can be addressed if encryption/decryption occurs at the TPM level and not via sharing keys.

3.4.1.2 Digital Twin

Digital twin refers to the digital representation of physical assets, processes, people, places, systems and devices that can be used for various purposes. In the context of the Cyber Security roadmap, this is an important area of technology as having a digital twin of complex systems, such as OT for CII sectors (e.g. power plants, subway control systems), IOT applications (e.g. smart sensors in hospitals, autonomous vehicles, smart building systems), would enable comprehensive and thorough analysis of the cyber resilience and security of these systems in the most realistic manner. Without a digital twin, it would be expensive to duplicate the same complex system physically for the tests and analysis; and it would be highly risky to conduct such activities on the production systems.

3.4.1.3 Data Diodes

A data diode is a unidirectional security gateway network appliance that allows data to travel just in one direction and that is used in guaranteeing information security. While data diode technology has been around for many years, since the 1990s, the category is still relevant in the roadmap.

The use of this technology at the edge of cyber physical systems in facilities such as nuclear power plants, electric power generation/distribution, oil and gas production, water/wastewater and manufacturing is important as legacy cyber physical systems may not be integrated with modern technologies in Cyber Security due to the inherent legacy design of systems.

In areas of other applications, there is a pressing need to develop suitable data diode solutions for cloud-based, virtualised environments, as well as highly complex IOT communications protocols.

3.4.1.4 Real-Time Monitoring & Threat Detection in CPS

There are many cyber event monitoring and inference commercial-of-the-shelf (COTS) software in the market for the enterprise environment. This does not translate directly to having the same in the CPS market as the protocols and behavioural mechanics of CPS systems are different from an Enterprise system.

Deployed systems contain many legacy systems which were not built to address security challenges. In this environment, event monitoring and inference technologies will need to be developed to effectively recognise anomalies in the CPS systems.

Current technology requires the human operator to make sense of the anomaly in CPS systems and the system design. In the last few years, research had been conducted to use historic logs and data to allow for automation in the detection of anomaly in CPS systems.

As a start, the Singapore Government has invested in these areas of research that use techniques of analysing historical data to in line behavioural analysis techniques in the past. These research outcomes are captured in research teams in NUS and SUTD. These research are prime for translation to enable CPS systems to start having automation in threat and vulnerability detection.

Cyber technology companies and cyber service companies providing Security Operation Centre services that intents to capture the CPS Cyber Security market can utilise these research outcomes to translate to capabilities within their product line.

3.4.2 3 to 5 Years

3.4.2.1 Access Management Framework to all Components in CPS

CPS provides an interesting challenge from the access and authentication perspective. CPS systems may be built by the integration of multiple subsystems from multiple vendors that uses different authentication and access systems.

With newer CPS system, there are already Authentication and access systems that are purpose built with high security as a consideration. But CPS systems also contain a lot of legacy systems that cannot be swapped out easily. There is a need to build an overlying technology layer that would account for the access and authentication needs for CPS systems that deploy a mixture of both legacy and new CPS technologies.

A common framework (including the tools to support) and protocols that would be able to serve as middleware to provide a security management framework would be needed to be able to support the security operations of CPS operators.

This would benefit CPS operators who have invested in technology from multiple vendors and are not in the process of technology refresh in the near term where they can consolidate and advance to newer systems that adhere to common security standards.

3.4.2.2 Software & Framework Extension to Digital Twin

There are increasing need for critical infrastructure (CI) operators, many of who are operating Cyber-Physical-Systems (CPS) to be subjected to government regulations in terms of cyber preparedness. There is a need to provide them with tools and services that would allow a comprehensive audit of these CPS systems.

As CPS systems are varied, they open up the possibilities of developing cyber audit tools to cater to the various sectors. Though the eventual tool could be varied, the underlying algorithm and methodology could possibly be abstracted to a higher level for research.

An example would be the development in software & framework extensions to the digital twin concept to support low-level simulation and high fidelity data generation of the CPS. Such extensions will support design, evaluation and integration of machine learning applications into CPS and support audit and incident response training.

In the longer 3 to 5 years' timeframe, these tools should be developed to be able to run automatically on a more periodic basis such that CPS can effectively be audited on the fly to provide a higher assurance level to the operators.

The expected stakeholders would be cyber audit tools developers/companies who can develop the tools to be used by security consultant companies who can provide cyber services to the CPS operators. CPS systems providers may also use such technology as a sales tools to upsell newer solutions to CPS operators.

3.4.2.3 Deception based Protection (in CPS)

Deception based Protection: CPS systems once deployed in production are typically out of bounds from any major upgrade or new initiative. These factors push them to be extremely susceptible to both

internal and external attacks (if a path can be found through to them). Any new protection mechanism can only be deployed in parallel to existing production environments. One such technology that is gaining traction is decoy based protection. This system has three architectural components.

a) Software based Simulation: This piece can study the behaviour of existing production systems non-intrusively and then replicate the behaviour to appear as the real system.

b) Alerting mechanism: Deployed decoys have the capability to run agents that can detect minute changes in its environment. When changes are detected alerts are raised. They also have the capability of sandboxing and detecting Indicators of Compromise for forensics and analysis.

c) Automated Polymorphism: The ability to constantly morph themselves so that they are not detected as decoys and to always maintain a higher level of vulnerability than the actual production environment so that they are attacked first before the production environment (easier access control using dictionary passwords, VLAN segregation with higher exposure to the internet, etc.)

3.4.2.4 Automation in Vulnerability Detection and Incident Response in CPS

The initial ability to be able to conduct vulnerability and initial appropriate defensive response in CPS systems would be expected to be available commercially. This would include methods in vulnerability discovery in embedded systems and detection of lateral movement and privilege escalation detection techniques in CPS.

Additional capabilities would be to have tools that would be able to automate the creation and testing of these created patches. Tools should be able to create the required compiled patch and to create a link that would enable the patch to intercept during run-time instead of the original embedded vulnerable firmware.

3.4.2.5 Data Protection and Security of Training Data

As the dependency on machine learning (ML) increases in the field of Cyber Security, one approach to compromise a system can come from the poisoning of training data so that ML generated models are flawed and thus fail to detect abnormal behaviours. Methods to be able to verify that training data and ML learning models are not tainted or compromised need to be developed so as to ensure that this is not a vector of attack that can be executed.

3.4.3 Beyond 5 years

3.4.3.1 Model-based Security Testing for Cyber-Physical Systems

Evaluating the security of cyber-physical systems throughout their life cycle is necessary to assure that they can be deployed and operated in safety-critical applications, such as infrastructure, military, and transportation. Most safety and security decisions that can have major effects on mitigation strategy options after deployment are made early in the system's life cycle. One of the methods to allow for a vulnerability analysis before deployment is in the use of well-formed models.

Verification techniques can include State-Space Exploration (model-checking, behavioural equivalences) and Compositional state space generation (Run-time verification, monitoring, and property enforcement)

3.4.3.2 Layered Defence

Layered Defence is a method for design and placement of dedicated CPS defence devices. Such defensive devices will serve a dual purpose: (a) they provide mechanisms to defend the cyber portion of a CPS as well as mechanisms that explicitly ensure the safety of each critical physical component of the CPS and of the system. These defensive devices need to be hardened against attacks, and provide reliable fail-safe mechanisms that allow a system to recover from attacks. In particular, such fail-safe mechanisms could be hardened sensors or fail-safe control devices.

3.4.3.3 Techniques for Automatic Patching of CPS Vulnerability

A much needed area of research in technology would be how vulnerability in CPS systems in operation can be detected and automatically patched. The current state of binary analysis and auto patching is progressing well but the techniques may be difficult to be implemented in CPS systems, especially when the CPS systems have not been designed to be patched easily while in operations.

3.4.3.4 Protocol-Oblivious Anomaly Detection in CPS

Current methods of network anomaly detection have focused on defining a temporal model of what is "normal," and flagging the "abnormal" activity that does not fit into this pre-trained construct.

This when applied to CPS traffic may be difficult as the protocols used in different CPS systems may differ and historical data to be able to create/flag abnormal behaviour is not easy to come by. Effective and efficient protocol oblivious methods to enable protocol anomaly detection data may need to be researched to enable more effective anomaly detection in CPS systems.

3.4.3.5 Lightweight & Resilient Crypto for Cyber-Physical Systems

Lightweight cryptography techniques and implementation have started to be translated into real world deployment. The drive to use these techniques is due to the lack of primitives capable to run on devices with very low computing power. Take for instance, RFID tags, sensors in wireless sensor networks or, more generally, small internet-enabled appliances that is flooding the markets in the age of Internet-of-Things (IoT).

But these cryptos are also susceptible to attacks and more research will need to be done to improve and lower the success rate of attacks.

3.5 Technology Adoption Readiness Map for Post Quantum Computing

Categories	NOW - 2 YEARS	3 - 5 YEARS	> 5 YEARS
Technology	Quantum random number generation (QRNG)		
	Quantum Key Distribution (QKD) (Free Space Terrestrial)	Quantum Key Distribution (QKD) (Satellite QKD)	Quantum Proof Cryptography

	Quantum Key Distribution (QKD) (Fibre QKD)	Quantum Key Distribution (QKD) (Terrestrial) Re-broadcast	Network QKD

Table 5: Technology Adoption Readiness Map for Post Quantum Computing

Post-Quantum technology enables organisations to protect their data against code-breaking quantum computers. This chapter of the cyber technology roadmap looks at the technology from Quantum Computing research that has practical usage in Cyber Security.

There is also a need to understand how quantum computing when actualised in the future would affect the cryptography that we use today. This is especially true when applied to data that are not time sensitive and would be affected by the advances made in quantum computing in the future.

The Singapore Government had invested in Quantum Computing research through the Centre for Quantum Technology (CQT). Interested parties are encouraged to collaborate with spin-off companies (e.g. S-Fifteen) that will license required IPs from NUS for commercialisation.

3.5.1 Now to 2 Years

3.5.1.1 Quantum Random Number Generation (RNG)

Quantum Random Number Generators (QRNGs) can be thought of as a special case of TRNGs in which the data is the result of quantum events. But unlike traditional TRNGs, QRNGs promise truly random numbers by exploiting the inherent randomness in quantum physics. A true random number generator provides the highest level of security because the number generated is impossible to guess.

3.5.1.2 Quantum Key Distribution (QKD) (Terrestrial)

Quantum key distribution (QKD) is a secure communication method which implements a cryptographic protocol involving components of quantum mechanics. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.

The security of encryption that uses quantum key distribution relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography, which relies on the computational difficulty of certain mathematical functions, and cannot provide any mathematical proof as to the actual complexity of reversing the one-way functions used. QKD has provable security based on information theory, and forward secrecy. This implementation can run over Free Space. This is available as an advance prototype currently. An alternative would be over untrusted network using fibre as long as the fibre cable is uninterrupted.

3.5.2 3 to 5 Years

3.5.2.1 Quantum Key Distribution (QKD) (Satellite)

Quantum Key Distribution through Satellite uses one or a few trusted satellites as relay stations to possibly to extend the distance of secure QKD to the global scale. Several experimentation including experiments with low earth orbit (LEO) satellites, have been conducted - 149, 150, 151, 152, 153, 154,

155. China, the EU and Canada are all currently exploring experimental ground-to-satellite QKD in ambitious long-term projects involving LEO satellites.

The studies in free-space QKD may also open the door to mobile QKD networks, which can be useful in many applications, such as ship-to-ship communication, airport traffic control, communication between autonomous vehicles, etc. In such a network, the mobility of QKD platforms requires the network to be highly reconfigurable—the QKD users should be able to automatically determine the optimal QKD route in real time based on their locations.

CQT had recently announced a partnership with a UK company that will provide the satellite bus and pointing system to integrate with CQT technologies to enable a satellite based product.

3.5.2.2 QKD (Terrestrial) Re-broadcast

For terrestrial implementation, there is a limitation of about 50km over uninterrupted cable for QKD to work. For implementation over larger distances, trusted relay needs to be implemented. By setting up trusted nodes, for instance, every 50 km, to relay secrets, it is possible to achieve secure communication over arbitrarily long distances. The QKD network currently under development between Shanghai and Beijing is based on this approach.

Another approach is quantum repeaters, which remove the need for the users to trust the relay nodes. Quantum repeaters are beyond current technology, but have been a subject of intense research efforts in recent years. Research efforts on quantum repeaters have focused on matter quantum memories and their interface with photonic flying qubits.

3.5.3 Beyond 5 years

3.5.3.1 Network QKD

QKD network structures must be considered in order to enable access by a greater many users and also to extend the reach and geographical coverage. In addition, the incorporation of mobile QKD nodes for key transports will add to network connection flexibility and allow even greater geographical coverage.

QKD technology faces a number of challenges such as distance, key generation rate, and practical security amongst other factors. QKD networks have a number of promising applications, for example, the development of secure distributed databases. First of all, they offer information-theoretic secure communications between nodes. Moreover, the generated keys can be used for continuous key renewal in the currently available symmetric cipher devices.

One of the most important challenges in the development of QKD networks is establishing secret keys beyond laboratory conditions. Thereby it is important to use a QKD protocol that guarantees secrecy in urban fibres with significant losses. This circumstance is one of the most important distinguishing factors of experiments on the quantum key distribution in urban conditions. It is also important to note that the post-processing procedures of sifted keys are an inherent part of QKD networks.

A hybrid approach being worked on by CQT where Key Management Systems can be used to provide inter-connectivity across networks by building on the existing QKD systems may see productisation within a 2 to 3 years' timeframe.

3.5.3.2 Quantum Proof Cryptography

Quantum-proof (aka quantum-safe or quantum-resistant) refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against an attack by a quantum computer. The

need for quantum safe cryptography is also dependent on the time sensitivity of the data to be protected.

Symmetric Algorithms

Grover's algorithm used in Quantum Computing is a method that gives a square root increase in efficiency for quantum computers running key searches. This essentially means that the fundamental of mathematics are not really addressed directly by the quantum computer and Quantum Computing is treated as running on a faster computer and the symmetric key algorithms are not broken in the way asymmetric algorithms.

This also means that symmetric key operations (like the AES) and cryptographic hash functions (SHA-2) will be impacted, but by lengthening the keys or resultant hash values, they can be made quantum safe.

Asymmetric Algorithms

As of 2018, this is not true for the most popular public-key algorithms, which can be efficiently broken by a sufficiently strong hypothetical quantum computer. The problem with currently popular algorithms is that their security relies on one of three hard mathematical problems: the integer factorisation problem, the discrete logarithm problem or the elliptic-curve discrete logarithm problem.

All of these problems can be easily solved on a sufficiently powerful quantum computer running Shor's algorithm. Shor's algorithm is a method by which a quantum computer could turn a cryptographically hard problem, like prime factorisation, into a problem that could be solved in a reasonable amount of time.

However, running a key search like this depends on the number of qubits the quantum computer has available, and this has been one of the scaling problems with the current commercial products. Research in the following areas should be tracked.

a) Lattice encryption/homomorphic encryption

b) Code-based encryption

c) Multivariate Public Key Cryptosystem (MPKC)

d) Supersingular elliptic-curve isogeny cryptography (SECIC)

3.6 Use Cases

3.6.1 Managed Security Services

Managed Security Service Providers (MSSP) serves an important function in the Cyber Security eco-system. Companies whose core business is not Cyber Security can leverage on services such as managed Security Operations Center (SOC) services to alleviate costs of recruiting and maintaining a big team of competent Cyber Security personnel.

Research in Machine Language (ML) and Artificial Intelligence (AI) can enhance the capabilities in this space. The adoption of ML and AI for security can be separated into 3 layers. First layer focuses on attack and defence techniques. Second layer focuses on AI in the use of modelling security and third layer on the development of secure architecture.

Managed SOC operators would need to look to at addressing the following challenges:

3.6.1.1 Increase Accuracy in Threat Detection

Beyond purchasing commercially available SOC products, SOC operators should look at investing in technology research in Machine Learning (ML) where contextual awareness and correlation in threat identification and behaviour modelling can be further improved. This will increase the accuracy of detection and reduce analysis fatigue. The ability to perform accurate sense making from multiple source of unstructured intelligence data would further improve the unique edge of SOC operators.

3.6.1.2 Recruitment and Retention of Capable Workforce

Capable Cyber Security manpower is a scarce resource which is required in managed SOC services. The research in the use of Machine Learning (ML) and Artificial Intelligence (AI) technology to efficiently conduct automated testing and verification (of alerts) and threat hunting can reduce the workload of the operators. Experienced operators can be given more senior technical roles over time with the increased efficiency of ML/AI enabled testing instead of manpower outflow due to the monotony of the role.

3.6.1.3 Making Cost of Subscribing to Such Services Affordable to Businesses

Cost of providing a managed SOC service correlates to the amount of Cyber Security manpower that is deployed to operate the service. Research that enables more efficient threat detection, identification and verification can reduce the heavy manpower deployed for these roles, which in turn reduces the cost of service provisioning and increases customer acquisition.

3.6.1.4 Enabling a Suite of Integrated Security Services to Maximise Protection and Efficiency

Cyber Security service providers would need to be able to provide an integrated suite of security services that would be able to ensure sufficient due diligence of cyber hygiene has been achieved. There may be a need to differentiate such service providers via pre-approved vendor schemes to demonstrate the level of competency.

3.6.1.5 Better Visual Representation of Data

The ability to present data and reports in an appropriate format to the appropriate stakeholders is an important capability that would create an impact. Investments in Natural-Language Processing (NLP) as applied to the SOC context would enable the presentation of data to be agile enough to show different aspects of security on different phases of the incident lifecycle.

The ability to automatically generate appropriate reports suited for “C” level management also helps to better justify the Return-of-Investment (ROI) for the adoption of the MSSP’s services.

3.6.2 Security as a Service (SECaaS)

Security as a Service would be an important aspect of the API Economy. Businesses building on top of different APIs would prefer to spend their time focusing on the most critical business task instead of worrying about Cyber Security. There is a need to be able to provide affordable cyber hygiene to business going digital.

The following SECaaS are identified as important areas which is required for Cloud Native Application.

3.6.2.1 Federated Identity Technologies

The ability for SECaaS operators to provide services to address the needs of businesses to manage Identity and Access management issues is increasingly relevant. By abstracting this IAM as a service, they take away the need for a business to know how to implement the protection mechanism of IAM services. As a longer term enhancement to such services, Key Management as a Service (KMaaS) can be further introduced to increase the security posture of businesses.

3.6.2.2 Cyber Health Checks

The ability to have independent 3rd parties being able to provide a continuous status of your internet facing businesses' cyber health provides businesses an understanding of the security performance of their Cyber Security investment in real time. Such SECaaS operators can leverage vulnerability discovery technologies to further improve upon their services.

3.6.2.3 Automated Security Orchestration

The ability to deploy and operate Cloud Native Applications securely depends on the ability of the DevOps engineers to understand and deploy the appropriate security orchestration such that the complex mechanism in which multiple APIs communicate with each other is secured. SECaaS which can provide automated security orchestration in continuous delivery would enable businesses and developers to concentrate on the technicalities of application development and deployment.

3.6.2.4 Native Cloud Application Endpoint (API) Threat Prevention

The APIs that would be used by the businesses would need to be continuously monitored for vulnerabilities and attacks. SECaaS services and abstract the threat detection mechanisms and trigger appropriate response to counter the threat.

3.6.2.5 Business Continuity/Disaster Recovery

Business Continuity and Disaster Recovery has theoretically become easier when application moved to the cloud and deploy services based on automated orchestration tools (e.g. Kubernetes). Business Continuity (BC) /Disaster Recovery as a Service (DRaaS) operators would need to be able to have technology that test the process of correctness of data backups, application aware replications and the frequent exercise of Disaster Recovery.

3.6.3 Security Consultancy Services

Security Consultancy coverage deals with a whole gamut of areas. From designing secure architectures, cyber assessment and audit services, cyber forensics, cyber validation. Cyber exercises, etc.

Technology used in this area will have at least the 3 benefits:

a) Reduce the manpower to discover and analyse issues

b) Reduce reliance of scarce resource of highly trained experts

c) Catalyses new areas of security consultancy in emerging areas.

3.6.3.1 Emerging Technology Cyber Forensics Services

Most global Cyber Security consultancies with an investigate arm would already have a forensics expertise service. The expertise and tooling required for this area of work is expensive due to the

expertise required to operate the tools and analyse the raw data extracted. With advance research in tooling and analysis of extracted data, we could potentially lower the cost via automation of certain process.

The forensics of emerging technology would also be an area of interest for the local based industry to collaborate and build expertise to serve regional and global markets.

3.6.3.2 Bug Bounty Cyber Security Services

Advances in binary analyse and vulnerability discovery technologies can expand the effectiveness of tools that used commercial products. This in turn can spur new services that leverage curated expertise from the Cyber Security community to help discover bugs and vulnerabilities early so that businesses can rectify these early.

3.6.3.3 Digital Twin Services

Digital Twin technology provisioned as services provides for a safe approach for businesses to simulate the integration of new technology into existing systems to check if there are any issues that need to be addressed as part of the integration before to full commitment. The usefulness of this service would be dependent on the fidelity in which the digital twin can be simulated.

3.6.4 Cyber-Physical Security Services

Most Cyber Security technologies and services are designed for information technologies (IT), which refers to the entire range of technologies for information processing. Meanwhile, operational technology (OT) Cyber Security is an emerging field. OT encompasses the hardware and software that detects or causes a change through direct monitoring and/or control of physical devices, processes and events.

In the past, OT systems were not connected to the internet and relied more heavily on physical security. However, with the growing use of Industrial Internet-of-Things (IIoT) and networked software, operational systems have become online and are increasingly exposed to cyber threats. This is integration is referred to as Cyber-Physical Systems (CPS).

Some of the key areas of importance and relevance to Critical Infocomm Infrastructure (CII) protection of CPS where the industry can build solutions and services are:

a) Monitoring, Detection and Defence Automation (e.g. Behaviour Analytics)

b) Attack Prevention (Using Deception Technology)

c) Assessment and Audit (Digital Twin Concepts)

d) Assets Discovery

Business who wants to enter this market with Cyber-Physical security offerings should take note of the key considerations for CPS security:

a) Maintaining control is the absolute top priority

b) Security cannot leave any negative impact (disruption, slowdowns, etc.) to operations of critical infrastructure

3.7 Contribution 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 be crucial to ensuring the success of the Cloud Native Architecture. Exhibit 7 below shows how some of the key Cyber Security technologies designed specifically for use with Cloud Native Architecture. Chapter 3.2 elaborates on this topic in more detail.

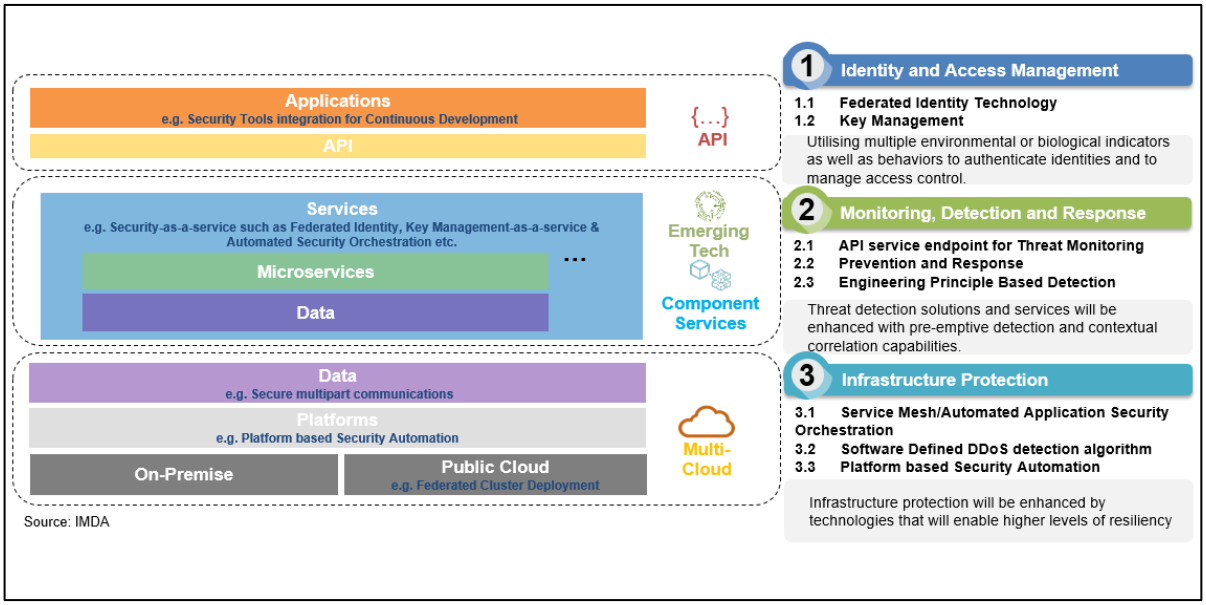

Exhibit 7: Contribution of Cyber Security to Cloud Native Architecture

4 SWOT ANALYSIS

For Singapore to experience the benefits of Cyber Security technologies, it is crucial to understand the strengths, weaknesses, opportunities and threats (SWOT) of enterprises and businesses. With this understanding, we can ensure that the findings are relevant to their needs and concerns.

The framework shown in Exhibit 8 allows for a well-rounded analysis of this matter, with the following key criteria; Market, IP & Talent, Capital, Infrastructure & Ecosystem, Policy & Regulations.

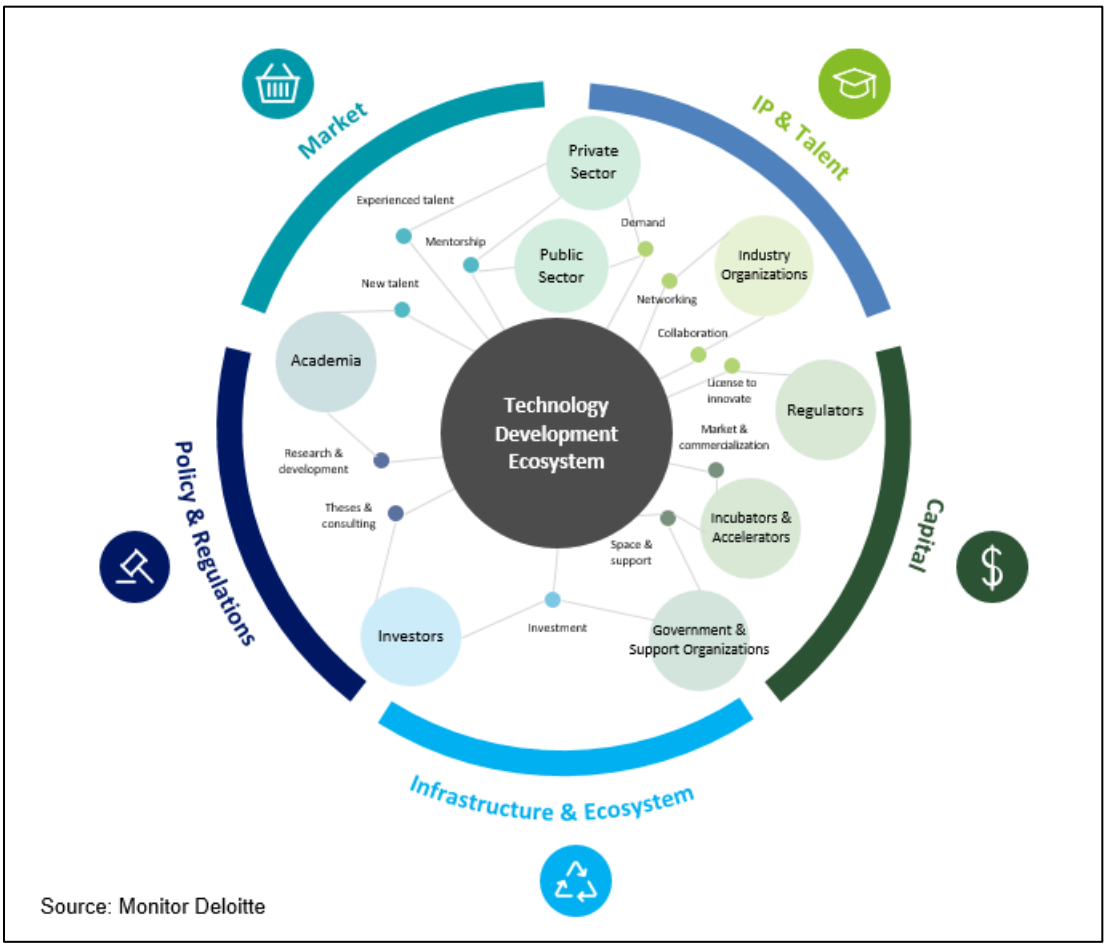

Exhibit 8: Framework for SWOT

A SWOT analysis of the Singaporean Landscape for Cyber Security revealed the following strengths, weaknesses, opportunities and threats clearly indicating the areas in which Singapore should expend resources in order to become a global player in the area of Cyber Security. Please refer to Exhibit 9 that provides a summary.

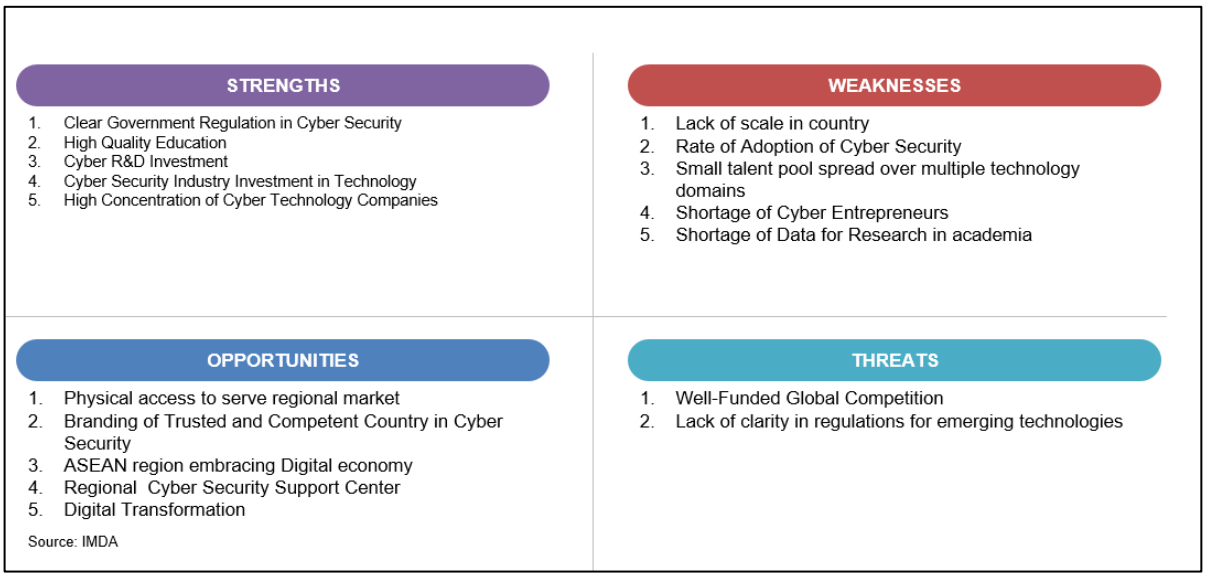

Exhibit 9: SWOT Analysis of Cyber Security

4.1 Strengths

4.1.1 Government Regulation – Cyber Security Act – Critical Infocomm Infrastructure Protection

The Singapore Government had laid out clear regulatory requirements for Critical Infocomm Infrastructure (CII) with regards to Cyber Security where critical infrastructure operators are required to adhere to. This opens up opportunities for CII cyber solutions/service providers to build up expertise in a market area that is growing due to the increase awareness of importance to the world.

4.1.2 High Quality Education

Cyber Security has been recognised as a growing area of importance for many years and Singapore has put in place curriculum in Polytechnics and Universities to educate a new generation of workforce to pipeline into the industry.

4.1.3 Cyber R&D Investment

Singapore has invested SG$130 million in the National Cyber Security R&D Program through NRF. There are further R&D investments by local Cyber Security players in corporate labs. These efforts enlarge the cyber Intellectual Property pool available to Singapore companies to exploit in technology innovation. Singapore Cyber Security research often find high quality collaboration partners in the U.S., Israel and Europe.

4.1.4 Cyber Security Industry Investment in Technology

Local Cyber Security industry has invested in Cyber Security through start-up incubation, venture capital investment and acquisitions.

4.1.5 High Concentration of Managed Security Service Providers (MSSP)

Singapore has attracted a high concentration of MSSP with our pool of highly (cyber) educated workforce. The nation has managed to attract most of the major MSSP providers to service regional

customers through Singapore. In doing so, Singapore is in a good position to encourage further innovation and Intellectual Property creation in Cyber Security capabilities and technologies used in these businesses.

4.2 Weaknesses

4.2.1 Lack of Scale in Country

Though Singapore has a highly addressable market as the country goes digital, it may not be sufficient to support a Cyber Security eco-system on its own. Singapore cybersecurity businesses needs to find innovative approaches to reach regional markets and beyond.

4.2.2 Rate of Adoption of Cyber Security

Though there are efforts in Cyber Security awareness, there are still room to improve the adoption of Cyber Security for the general population and local businesses, especially the SME market.

As more businesses turn digital, increased awareness of how businesses would be affected by the adverse consequences of Cyber Security incidents will need to be inculcated into the business consciousness so that businesses will implement good Cyber Security by design and practice good Cyber Security hygiene.

4.2.3 Small Talent Pool Spread over Multiple Technology Domains

Singapore has a talent pool that has to spread over many technical domain of importance, thus shrinking the available talent for Cyber Security work. A small pool of experts also mean that this is a very expensive pool of talent to maintain.

4.2.4 Shortage of Cyber Entrepreneurs

There is a shortage of cyber entrepreneurs in Singapore as cyber innovation requires very niche expertise. There is limited outflow from research institutions taking on the entrepreneurial path. There are also shortages of trained people who are able to understand and act as a bridge between research outcomes and industry commercialisation of products.

4.2.5 Shortage of Data for Research for the Institute of Higher Learning (IHL)

There is a shortage of data available to the IHLs to conduct their research validation due to the difficulty of sharing such data from government or private organisations. This impedes research from further improvement and being as close to reality as possible.

4.3 Opportunities

4.3.1 Physical Access to Serve Regional Market

Singapore serves as a good springboard to regional markets. Travel from Singapore to serve an addressable regional market is within a 6-hour flight.

4.3.2 Branding as a Trusted and Competent Country in Cyber Security

Singapore is considered a trusted and competent Cyber Security thought leader in the ASEAN region.

4.3.3 ASEAN Region Embracing the Digital Economy

The ASEAN regional is in a digital growth spurt with many countries preparing for the digital economy. This opens up the regional market for competent Cyber Security service providers.

4.3.4 Regional Cyber Security Support Centre

Singapore is geographically located in a location that is suited to be a service provider in a “follow the sun model”. Given the highly educated population and big investment in technologies in Managed Security Services, Singapore is in an advantageous position to capture a bigger share of this market.

4.3.5 Digital Transformation

Digital transformation of Singapore provides a unique opportunity to open up a bigger addressable market that Cyber Security solutions and services providers can reach. The majority of businesses in a single market would consist mostly of Small and Medium Enterprises (SME). If local Cyber Security companies are able to succeed in strategies to reach this portion of the market, it can easily expand to regional markets with the same services.

4.4 Threats

4.4.1 Well-funded Global Competition

Cyber Security is a hugely addressable market due to its impact on the digitisation of the world. This has spurred well-funded global competition globally where Venture Capitals are willing to invest in cyber start-ups with emerging technology that solves tomorrow’s problems.

4.4.2 Lack of Clarity on Regulations on Emerging Technology

There is a lack of clarity in how different emerging technology would be regulated. This makes it difficult to make investment decisions on the development of associated Cyber Security technologies for these emerging technologies as the possible return of investment may be difficult to gauge.

4.5 Conclusions from SWOT analysis

In conclusion, 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 other 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 innovation hubs and local research institutes, aiming to meet increasing demands from global and local Cyber Security players. Furthermore, existing initiatives such as Smart Nation initiative could be leveraged to make Singapore as a hub for emerging technologies, encouraging collaborative efforts across the region.

Singapore also needs to continue providing a favourable environment with government support, necessary regulatory and legal framework, which ultimately can help Singapore to lead the fast-moving tech advancement.

5 RECOMMENDATIONS

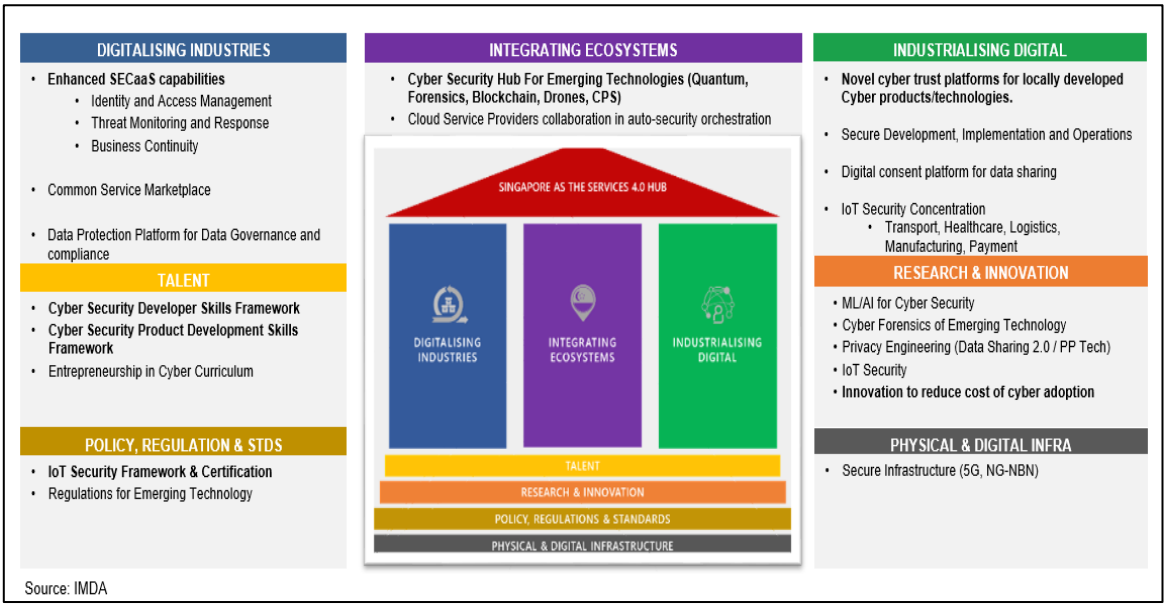

Exhibit 10: Alignment of Recommendations in Cyber Security Technologies to DE Framework

Based on the guidelines developed from the SWOT analysis of Singapore Landscape, 6 main recommendations have been identified, which will be further elaborated in this chapter:

a) Cloud Native- Everything-as-a-service

b) Privacy Engineering and Protection

c) Internet-of-Things (IoT) Cyber Security

d) Cyber Security Hub for Emerging Technology

e) Awareness, Adoption and Ecosystem Development

f) Pathways to Technology Commercialisation

5.1 Cloud Native – Everything-As-A-Service

In IMDA's push for Cloud Native – Everything-As-A-Service, the Cyber Security services that would complement the approach would need to be ready. Findings from a survey conducted by Capsule8 indicated that Cyber Security is the biggest barrier for a Cloud Native approach for their business. Data protection technologies should also be a key focus given that data is a key asset of business in the digital economy.

5.1.1 Cloud Delivered Application Security

The Government should catalyse the availability of cloud delivered application security for Cloud Native Applications. As businesses go digital, the cyberattack surface of businesses also increases proportionally. Prevention, Monitoring, Detection, Response and Recovery type of Cyber Security services should be readily available at an affordable cost to digital businesses.

5.1.2 Identity, Authentication and Access (IAM)

One of the key building blocks of a Cloud Native Application is the IAM component. The Government can catalyse IAM Cloud Services to abstract businesses from having to worry about the technicalities of securing identity services so that they can concentrate on their core capability of their business.

Although through the use of Federated Identity technologies end users would be able to leverage their social media accounts for login to services, the use of these accounts would still be subjected to account provider's (e.g. social media companies) terms of service.

Preference would be to have local IAM service providers, so that business can set their own terms of use in accordance to the contractual agreement with IAM service providers. The Government can consider catalysing these through existing authentication providers, National Digital Identity (NDI) or through new cyber start-ups in this space.

5.1.3 Need for Cloud Security Orchestration

The move towards a Cloud Native approach to working necessitates the training of staff on DevOps, which focuses on the development of an application and how it can be deployed in a continuous integration model. An often overlooked area is the integration of security orchestration in this area. Thus, an emerging area of DevSecOps is the ability to do continuous development/continuous integration in a secure manner.

DevOps engineers would need to be trained in DevSecOps. In the longer term, we should look at technology advances that would abstract security orchestration through automation such that DevOps engineers can concentrate on their core capabilities of development and integration.

Collaboration with Cloud Service Providers (CSP) in advancing cloud security orchestration technologies would benefit digital businesses.

5.1.4 Common Service Marketplace

A common marketplace for Everything-As-A-Services will need to be established with a specific chapter on Cyber Security services.

For the Cyber Security services listed, it would need to have comprehensive documentation on how the Cyber Security service would integrate with typical Cloud Native applications such that there is no ambiguity on the challenge of integration of such services. Being able to see the ease of integration of such services would allow SMEs to jumpstart their digital transformation.

With the services catalogue in place, businesses will also be able to see what will be needed as part of their digital transformation. Affordability of the cyber service to a non-cyber digital business should be a factor for inclusion to the marketplace.

5.2 Privacy Engineering and Protection

In the context of the digital economy, privacy engineering and protection is not just about being able to meet Singapore's Personal Data Protection Act (PDPA). As digital businesses operate across borders and customers can be of any nationality and data regulations (e.g. GDPR) beyond Singapore can affect digital businesses.

5.2.1 Research in Privacy Engineering

As Singapore is a hub for the inter-connectivity in this region, there will be a huge amount of data passing through Singapore. It is natural for big data analytics to be applied to discover and extract meaningful information and insights for use in many areas. However, data privacy remains a challenge

for such data to be used and there arises a need to explore how to preserve data privacy and yet "work with data" simultaneously.

Privacy technologies that are scalable and can support privacy engineering operationally are still few and far between. This is an area that would require research institutes and the industry to work closely together to find commercially viable solutions to today's data privacy challenges.

The capability to enable privacy preserving data sharing will not only open up the digital economy to better services, it would also allow for greater collaboration between the industry and research community.

With better and bigger data sets that can be shared securely between businesses and research communities, the opportunity to create Intellectual Property that can power even greater capabilities will be boosted. It is recommended that the Government invest in privacy engineering research and technologies that have a high probability of commercialisation.

5.2.2 Digital Economy Tools to Encourage Data Sharing

The businesses in the digital economy will generate a lot of (consumer) data. Similarly, digital businesses are looking for more data to better serve their customers or to make a decision on customer acquisition.

In the absence of highly scalable data-sharing privacy tools, an alternative would be a data consent service/platform that will put the decision to share the consumer's data in the consumer's hands. These data consent services can be implemented via APIs that businesses access. An example implementation can be seen in the "Data Empowerment and Protection Architecture (DEPA)" (indiastack.org).

5.2.3 Technology for Compliance to Data Regulation

Businesses are responsible for compliance to data protection and regulations. Small businesses may not have the technical knowledge or the capital cost to invest in privacy protection technologies to meet the requirements of regulation.

Platforms or services that can be used by small businesses to abstract themselves from worrying about compliance of data protection regulation as long as they are operating on the platform or using those data protection services would help in digital transformation of the economy.

5.3 Internet-Of-Things (IoT) Cyber Security

5.3.1 IoT Cyber Security Framework

The report recognises that there are multiple parties in the global ecosystem trying to address the issue of setting Cyber Security standards in IoT. An example would be Singapore's effort in TR64 - Guidelines for IOT Security for Smart Nation. All of these try to address IoT Security from different aspects of the deployable IoT Solution.

A framework for IoT Cyber Security will need to be established to identify and inform buyers of Cyber Security concerns in each aspects of the IoT product lifecycle from development, acquisition to decommission.

From a longer term perspective, technological tools will need to be developed to automate this process. It may be worth engaging the industry to understand which layer of the entire stack in IoT would benefit from regulatory requirements.

5.3.2 Areas of Concentration for IoT Cyber Security

It is also recommended that efforts in commercialising IoT security products should concentrate on the higher levels of the IoT stack (e.g. applications) where IoT Cyber Security solutions are still nascent and can be introduced as part of the IoT deployment.

A key application area would be in the use of IoT devices for secure payment services. It is recognised that IoT devices' ability to introduce modular security components are still limited at this stage in time.

The polling results from a local Cyber Security industry engagement session of "C" level personnel indicated that the Transportation, Healthcare, Logistics and Manufacturing sectors as having the highest potential of success for a IoT Cyber Security business due to industry presence and government and foreign investments opportunities.

From a technology perspective, the most useful and urgent capability required would be a rapid way to detect and identify devices joining the IoT network and to be able to quickly response to any rogue devises discovered. This asset management database would also enable incident management and investigation when required.

5.3.3 IoT Identity Management of Assets

The value of the capability brought about by IoT is not limited to activities conducted within the borders of a single country. As a result, secure device identity technology that can work across borders play an important role in enabling the benefits that can be brought about by IoT.

eSIM is not only a connectivity enabler but also a form factor of certificate for device identification. The way it is provisioned securely is an important technology that should be taken into account. The ability to be compatible with international telco networks is important and moreover, for security and economic reasons, a domestic standard is critical for the national deployment and management of IoT security.

5.4 Cyber Security Hub for Emerging Technology

Establishing Singapore as a Cyber Security hub for the region has the benefits of being able to attract more Cyber Security talent to collaborate with Singapore and establish local businesses. Singapore has invested in Cyber Security research in multiple areas. Being a cyber-technology authority hub would be important to further solidify our reputation in Cyber Security.

It is recommended that the Government study the possibility for Singapore to excel in some of these Cyber Security for emerging technology to put Singapore in a leading position in these cyber technology areas. Factors to consider would include research capabilities, talent pipelining, industry willingness to collaborate, possible markets and global competition in the domain.

5.4.1 Cyber Investigation Tools of Emerging Technology

There are many emerging technologies that are being adopted in our effort to leverage technology in digitally transforming our industry. The area of cyber forensics of emerging technology research and tooling, would be one such area where there is no dominant hub on the global stage. Singapore has invested in research on multiple areas of forensics for emerging technology which should be leveraged to build a position of authority in these areas. Examples of which are multimedia and drone forensics.

In the E-payment domain, the ability to conduct rapid investigations would aid in early fraud detection. Similarly, in the domain of blockchain, the ability to conduct forensic studies on the blockchain can verify whether anyone is trying to manipulate the blockchain with known attacks against blockchain proof mechanisms.

5.4.2 Blockchain Cyber Security

Singapore is in a unique position where blockchain technology companies are moving here to work on their blockchain implementation due to the forward-looking regulatory framework for this technology in the country. This provides Singapore technology a good pool of collaborators to work within developing, testing and validating blockchain Cyber Security solutions.

5.4.3 Cyber Physical Systems Security

Within corporate and investment activities, cyber-physical security is not lacking attention as well. Last year, PAS, a leading provider of industrial control system cyber-physical security raised US$40 million growth investment from Tinicum, a private investment firm.

Singapore has invested heavily in research for Cyber-Physical Systems Cyber Security, particularly in Singapore University for Technology and Design (SUTD) and I2R, A*Star. Technology advances from these research institute have been proven through competitions to be on par if not better than current solutions in the same problem space.

There are local companies trying to commercialise these research outcomes. Singapore had invested heavily in cyber research and research infrastructure in the Water, Power, Transport and Manufacturing Sectors. We should leverage our expertise built up in these areas for translation and commercialisation.

To be able to sustain the expertise and capabilities in Cyber-Physical Systems Cyber Security beyond just the research community, Singapore should explore interventions which would help open regional and global market pathways for the Cyber-Physical Systems Cyber Security industry.

5.4.4 Quantum Technologies

Singapore's investment in Quantum Technologies is producing research outcomes that are comparable to world class research organisations. There are also efforts to translate technologies such as Quantum Random Number Generations (QRNG) and Quantum Key Distribution (QKD) into commercially viable products. Singapore can further leverage upon the expertise built up through quantum research to develop quantum sensors and equipment that can be used in quantum security implementation.

It is recommended that the Government collaborate with the industry to present open showcases of the use of quantum security technologies and to work with service providers to develop viable quantum key distribution services.

5.5 Awareness, Adoption and Ecosystem Development

Cyber Security awareness is still not embedded into the deep consciousness of the general population. The person on the street is still unable to internalise the negative effect of a Cyber Security attack on their own lives. In the Small and Medium Enterprise (SME) business sector, the cost of adoption versus the likelihood of their business being adversely affected by a Cyber Security attack is still being debated.

It will require a concerted effort by skilled professionals to attempt to "simplify" the matter for the general public to understand, accept and be part of the effort to counter any cyber threats.

5.5.1 Grooming of Cyber Entrepreneurs

Beyond the deep Cyber Security technology that needs to be developed, we would also need to be able to groom entrepreneurs who can create innovative, simple and affordable products and services

to be taken up by the masses in Singapore and beyond. This is essential to catalyse mass adoption and sustain our resiliency to cyber threats and enable our vision for Smart Nation.

5.5.2 Cyber Secure Infrastructure

To be able to continue to attract regional business to host their E-Services, IT or e-commerce service in SG, we need to operate top-notch communication and cloud infrastructure to attract such businesses.

To do this, we need (1) strong Cyber Security practices in governing the infrastructure businesses, (2) strong disaster recovery capability to provide redundancy to that infrastructure, (3) a strategy to groom local talent in creating innovative and attractive services, including Cyber Security products and services, which can attract services and data to be hosted in Singapore.

It is recommended that the Government explore novel approaches to build trust in the Cyber Security products developed in Singapore. A possibility is in the provision of an insured liability model in which locally developed accredited Cyber Security products can be insured against cyber vulnerability such that the end user interest can be protected.

5.5.3 Cyber Security Development Talent

The focus of Cyber Security talent pipelining is currently concentrated in fulfilling the operational needs of Cyber Security. We will also need to be cognisant of the fact that the Cyber Security ecosystem spans from the development of secure products to the implementation and operations of the Cyber Security systems. The skillsets required for Cyber Security product development is different from Cyber Security operations.

The Government had invested in Cyber Security research with the intention that the research outcome can be translated by the industry into commercially available capabilities. The challenge for Singapore is in the shortage of talent in

a) Scouting and understanding novel Cyber Security concepts for product development

b) Managing Cyber Security product development

c) Technical development capabilities to develop Cyber Security products

d) Secure software development capabilities

For Singapore to be able to create innovative Cyber Security products as part of the Cyber Security eco-system that Singapore is building, there is a need to consider the development of a talent supply pipeline to ensure that the manpower capabilities in engineering and operations support required for different aspects of the end-to-end cyber technologies and capabilities are available.

It is recommended that the Government work with the industry and academia to define the skillsets and career pathways of talent supply in this area to enable Singapore to harness the full benefits of the investment that we have put into Cyber Security research.

5.6 Pathways to Technology Commercialisation

There are various pathways that enterprises or academic/research institutions can embark on to accelerate the commercialisation of technologies.

5.6.1 Allowing Research Spin-offs and the Bridging of Research & Commercialisation

Allowing spin-offs, universities, research & development centres and Centre of Excellences can enable technology transfer from research to commercial. University of New Brunswick (UNB) is an example which has created multiple spin-off Cyber Security companies.

Among them, efforts by a part-time student cum technical specialist to reduce hostile attacks on the university's computer network led to the development of intrusion detection technology. The spin-off, Q1 Labs, was later acquired by IBM in 2011 and has been used in IBM's offerings.

Technology transfer and commercialisation requires different capabilities than those required for research and development. Universities and research institutes can overlay their academic research environment with an infrastructure that is more common to a high-technology company.

For example, The Centre of Secure Information Technologies (CSIT) at Queen's University Belfast co-locates their commercial and engineering staff alongside academic research teams. They can provide the research teams with strong market awareness by supporting industry engagement, creating prototypes and delivering engagement with businesses and industry.

5.6.2 Building a Global Cyber Security Community

A Cyber Security community that is open and includes a wide range of stakeholders, can identify, evaluate and position to capture value from evolving market opportunities efficiently. With a community in place, a process then can be used to convene a systematic iterative approach to understanding the values of technologies and how to commercialise it for full impact.

This community should also be connected to a larger global Cyber Security community, for example, the Global Ecosystem of Ecosystems Partnership in Innovation and Cyber Security (EPIC) has gathered 24 independent ecosystems from across the globe, including prominent security clusters such as CyberSpark and Hague Security Delta. Their key activities are defined by 10 key areas: networking, projects, talent, exchange, evaluation, content, emerging, advocacy, investment, and standards.

The approach to building a Cyber Security community can include:

Multilateral partnerships on Cyber Security testbeds - Businesses and academic/research institutions, can form partnerships, along with local and foreign governments and Cyber Security hubs on Cyber Security testbeds. This will attract MNCs to test their technologies in Singapore, or enable them to test Singapore's home-grown technologies within their organisations.

Europe's largest security delta, Hague Security Delta has realised the value of building a testbed for multilateral collaboration. Its National Cyber Testbed initiative that is underdoing evaluation, will allow for cooperation with foreign testbeds for research & development, awareness, training, standards, and norms. Similarly, Singapore's National Research Foundation had funded the development of the National Cyber Security Laboratory for R&D and collaboration purposes. The platform can be opened up to Industry players to carry out more extensive and cross-sector testing.

Cross-border research partnerships - Businesses and universities or research institutions can also engage in a partnership, or invest in other entities with existing capabilities to enhance their own Cyber Security capabilities. The National Research Foundation actively finds opportunities to allow the local Universities and Research Institute to collaborate with world class Cyber Security research institutes.

Public-private partnership on Cyber Security accelerator - Industry, universities and government can partner on launching accelerators to foster innovation and entrepreneurship within local Cyber Security communities. Part of New York City Economic Development Corp.'s Cyber NYC initiative to foster public-private partnerships, they are launching the city's first Cyber Security accelerator. The accelerator will act as an incubator for start-ups by connecting them with local universities and industry.

6 SUMMARY

As a digital economy enabler, Cyber Security is required in every sector that is part of the digital economy. It needs to be considered in every aspect of technologies that businesses intend to deploy as part of their service offerings. The key aspects of Cyber Security technologies in this context would be to encourage business adoption of common Cyber Security technologies as foundation services for their businesses. This can be done through

a) Developing (or catalysing) relevant Cyber Security services that can be adopted via an API implementation as part of the Cloud Native approach for digital businesses to leverage on.

b) Using technology to make Cyber Security services affordable for the average digital business.

c) Exploring the development of Cyber Security services platforms that can provide an abstraction layer such that it enables digital business owners to focus on their core capabilities

With aspirations to be key players in the domains of Cyber Security, companies need to continue to be relevant in the new operating paradigm and provide top notch cyber services and solutions based on the ability to innovate in the global economy, we would need to

a) Identify the gap in skillsets in innovation and translation to commercialisation so as to develop or enhance development programs

b) Explore and experiment with new ideas and platforms to enable more translation of research for commercialisation

c) Leverage Singapore's highly trained talent and trusted reputation to propel the local Cyber Security industry to expand regional and globally.

APPENDIX A: GLOSSARY

TECHNOLOGY	GLOSSSARY
3GPP	The 3rd Generation Partnership Project (3GPP) unites seven telecommunications standard development organisations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organisational Partners" and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies. The project covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, and quality of service - and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks.
Augmented Reality	AR overlays digital information on real-world elements. Augmented reality keeps the real world central but enhances it with other digital details, layering new strata of perception, and supplementing your reality or environment.
Cyber-Physical Systems	Cyber-Physical Systems (CPS) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas.
Cryptography	Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorised user, allowing it to be transmitted without unauthorised entities decoding it back into a readable format, thus compromising the data. Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified. Cryptography is also known as cryptology.
Distributed Denial Of Service (DDoS)	A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilising multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up with highway, preventing regular traffic from arriving at its desired destination.

DevSecOps	The simple premise of DevSecOps is that everyone in the software development life cycle is responsible for security, in essence bringing operations and development together with security functions. DevSecOps aims to embed security in every part of the development process. It is about trying to automate core security tasks by embedding security controls and processes early in the DevOps workflow (rather than being bolted on at the end). For example, this could be the case when migrating to microservices, building out a CI/CD pipeline, compliance automation or simply testing cloud infrastructure.
Device Identifier Composition Engine (DICE)	DICE stands for Device Identifier Composition Engine, and it is a security standard created by the Trusted Computing Group (TCG) which has been addressing security issues for years. TCG announced the establishment of DICE Architecture, or DICE Architecture Work Group to address the need for increased security in the Internet-of-Things (IoT) therefore targeting products such as MCUs and systems on a chip (SoCs). DICE Architecture is a simple yet new security approach that doesn't increase silicon requirements, and it can be implemented in the hardware of security products during manufacturing. DICE Architecture explores new security and privacy technologies applicable to systems and components where traditional Trusted Platform Modules (TPM) may be unfeasible in IoT applications due to limitations related with cost, power, physical space, etc.
Enhanced Mobile Broadband (eMBB)	eMBB is a natural evolution to existing 4G networks that will provide faster data rates and therefore a better user experience than current mobile broadband services. However, it will go beyond merely faster downloads to provide an increasingly seamless user experience that will eclipse the quality of service we currently enjoy from fixed broadband technologies. Ultimately it will enable 360o video streaming, truly immersive VR and AR applications and much more.
Internet Engineering Task Force (IETF)	The Internet Engineering Task Force (IETF) is the premier Internet standards body, developing open standards through open processes. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Kubernetes	Kubernetes is an open-source system for automating deployment, scaling, and management of containerised applications. It groups containers that make up an application into logical units for easy management and discovery. Kubernetes builds upon 15 years of experience of running production workloads at Google, combined with best-of-breed ideas and practices from the community.
Machine Type Communications (MTC)	Machine Type Communications are about enabling direct communications among electronic devices, dubbed MTC devices, and/or enabling communications from MTC devices to a central MTC server or a set of MTC servers. Communications can use both wireless and fixed networks.

Message Queuing Telemetry Transport (MQTT)	MQTT is a machine-to-machine (M2M)/"Internet-of-Things" connectivity protocol. It was designed as an extremely lightweight publish/subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium. For example, it has been used in sensors communicating to a broker via satellite link, over occasional dial-up connections with healthcare providers, and in a range of home automation and small device scenarios.
Open Web Application Security Project (OWASP)	The Open Web Application Security Project (OWASP) is a 501(c) (3) worldwide not-for-profit charitable organisation focused on improving the security of software. Our mission is to make software security visible, so that individuals and organisations are able to make informed decisions. OWASP is in a unique position to provide impartial, practical information about AppSec to individuals, corporations, universities, government agencies and other organisations worldwide. Operating as a community of like-minded professionals, OWASP issues software tools and knowledge-based documentation on application security.
Quantum Cryptography	Quantum cryptography, also called quantum encryption, applies principles of quantum mechanics to encrypt messages in a way that it is never read by anyone outside of the intended recipient. It takes advantage of quantum's multiple states, coupled with its "no change theory," which means it cannot be unknowingly interrupted.
Security Operation Center (SOC)	A security operations centre (SOC) is a facility that houses an information security team responsible for monitoring and analysing an organisation's security posture on an ongoing basis. The SOC team's goal is to detect, analyse, and respond to Cyber Security incidents using a combination of technology solutions and a strong set of processes. Security operations centres are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organisational incident response teams to ensure security issues are addressed quickly upon discovery. Security operations centres monitor and analyse activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analysed, defended, investigated, and reported.
Software Defined Network (SDN)	The physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices. Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The OpenFlow protocol is a foundational element for building SDN solutions.

Transmission Control Protocol (TCP)	TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules defining the Internet.
User Datagram Protocol (UDP)	UDP is a communication protocol used across the Internet for especially time-sensitive transmissions such as video playback or DNS lookups. It speeds up communications by not requiring what's known as a "handshake", allowing data to be transferred before the receiving party agrees to the communication. This allows the protocol to operate very quickly, and also creates an opening for exploitation.
Ultra Reliable Low Latency Communications (uRLLC)	Services for latency sensitive devices for applications like factory automation, autonomous driving, and remote surgery. These applications require sub-millisecond latency with error rates that are lower than 1 packet loss in 10^6 packets.

APPENDIX B: REFERENCES

[1] "Market Definitions and Methodology: Software." Gartner. February 2018. https://www.gartner.com/doc/3855707/market-definitions-methodology-software

[2] The Global Risks Report 2018 13th Edition." World Economic Forum. 2018. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

[3] Hurst, Jeremy. "Harnessing the Cyber Security Opportunity for Growth." Deloitte, Ontario Centres of Excellence, and Toronto Financial Services Alliance. October 2016. http://www.oce-ontario.org/docs/default-source/publications/final_oce_tfsa_cyber-innovation-report_v6-2.pdf?sfvrsn=2.e

[4] Galletto, Nick, Global & Canada, and Global and Canada Cyber Risk Services. "Take the Lead on Cyber Risk" Deloitte. September 2017. https://www2.deloitte.com/global/en/pages/risk/articles/take-the-lead-on-cyber-risk.html.

[5] "Cyber Security Threats to Cost Organisations in Singapore US$17.7 Billion in Economic Losses." Singapore News Center. May 2018. https://news.microsoft.com/en-sg/2018/05/18/cyber security-threats-to-cost-organisations-in-singapore-us17-7-billion-in-economic-losses/.

[6] "Forecast: Information Security, Worldwide, 2016-2022, 1Q18 Update." Gartner. May 2018 https://www.gartner.com/doc/3875867/forecast-information-security-worldwide-.

[7] "Cyber Security Market: Growing to the Need of the Hour." Netscribes. October 2018. https://www.netscribes.com/cybersecurity-market-growing-to-the-need-of-the-hour/

[8] Gartner Market Databook, 2Q18 Update." Gartner. July 2018. https://www.gartner.com/doc/3883293/gartner-market-databook-q-update

[9] World Economic Outlook Database April 2018." International Monetary Fund. April 2018. https://www.imf.org/external/pubs/ft/weo/2018/01/weodata/index.aspx.

[10] "IDC Canada Releases Its 2018 ICT Predictions." International Data Corporation. December 2017. https://www.idc.com/getdoc.jsp?containerId=prCA43301517

[11] "Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures." Atlantic Council. September 2015 http://publications.atlanticcouncil.org/cyberrisks/

[12] "Trustwave Bolsters Detection & Response with New Proactive Threat Hunting Service." Trustwave. February 2017. https://www.trustwave.com/Company/Newsroom/News/Trustwave-Bolsters-Detection---Response-with-New-Proactive-Threat-Hunting-Service/.

[13] "2018 Cost of a Data Breach Study: Global Overview." Ponemon Institute. July 2018. https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

[14] "2018 Trustwave Global Security Report." Trustwave. April 2018. https://www2.trustwave.com/GlobalSecurityReport.Trustwave Global Security Report."

[15] IBM X-Force Threat Intelligence Index 2018. April 2018.https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=77014377USEN

[16] "Banks Spend on IT Security is 3x Higher Than Non-Financial Organizations" Kaspersky Lab.March 2017.https://www.kaspersky.com/about/press-releases/2017_banks-spends

[17] Lee, Jamie. "MAS to Raise Requirements on Cyber Resilience in Financial Sector." The Straits Times. May 2018. https://www.straitstimes.com/business/companies-markets/mas-to-raise-requirements-on-cyber-resilience-in-financial-sector

[18] Tham, Irene. "SingHealth Cyber Attack: Pause on Smart Nation Projects Lifted; 11 Critical Sectors Told to Review Untrusted External Connections." The Straits Times. August 2018. https://www.straitstimes.com/singapore/singhealth-cyber-attack-pause-on-smart-nation-projects-lifted-11-critical-sectors-told-to.

[19] "Norton Cyber Security Insights Report Global Results 2017." Norton by Symantec. 2017. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

[20] "2018 Identity Fraud: Fraud Enters a New Era of Complexity." Javelin. February 2018. https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

[21] Kuchler, Hannah. "Facebook Reveals Cyber Attack Affecting up to 50m Users." Financial Times. September 2018.https://www.ft.com/content/c5f13f30-c33f-11e8-8d55-54197280d3f7. Facebook reveals cyberattack affecting up to 50 million users

[22] Kwang, Kevin. "SingHealth Cyberattack the Work of Sophisticated, Usually State-linked Attackers: Iswaran." Channel NewsAsia. August 2018. https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-usually-state-linked-attackers-iswaran-10592762.

[23] "2018 Reform of EU Data Protection Rules." European Commission - European Commission. April 2018. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

[24] "National Cyber Security Strategy-2016-2021." United Kingdom Government. 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

APPENDIX C: WORKGROUP MEMBERS

Prof. Lam Kwok Yan (Co-Chairman of Workgroup 3)	Programme Chair (Secure Community), Graduate College Professor of Computer Science, School of Computer Science and Engineering, Nanyang Technological University (NTU)
Mr. Lin Yih (Co-Chairman of Workgroup 3)	Director, Digital Applied Research & Technology Pte. Ltd. (DART)
Mr. Lim Soon Chia	Director, Cyber Security Agency
Mr. Keng Seng Wei	Managing Director, DBS Bank, Infrastructure Management and Information Security Services, Technology Services, Group Technology & Operations
Mr. Chai Chin Loon	Senior Director, Government Cyber Security Group, Government Technology Agency
Mr. Hoo Chuan Wei	Chief Cyber Security Technology Officer, ST Electronics
Dr. Vrizlynn Thing	Senior Vice President, ST Engineering Head, Cyber Security Strategic Technology Centre
Dr. Li Tieyan	Huawei Security Expert, Huawei Singapore
Mr. Karthik Ramanathan	Senior Vice President, MasterCard
Mr. Lucas Lim	Senior Vice President, Asia Retail Innovation Department, Asia Growing Markets Division, Sumitomo Mitsui Banking Corporation
Ms. Karen Teh	Senior Deputy Director, National Cyber Security R&D Directorate

Mr. Jason Ho	Chief Executive Officer, Taisys Solutions Pte. Ltd.
Mr. Douglas Tang	Chief Executive Officer, Verint Systems (Singapore) Pte Ltd
Dr. Ong Chen Hui	Director, Singapore Telecommunications Limited (Singtel)
Mr. Kiren Zachariah	Vice President, Subex (Asia Pacific) Pte Ltd
Mr. Martin Khoo	Director, Cyber Security Management, Infocomm Media Development Authority
Mr. Jerry Khoo	Executive Manager, Infra Protection & Assurance, Infocomm Media Development Authority
Mr. Bernard Low	Manager, Infra Protection & Assurance, Infocomm Media Development Authority