Unlocking the cybersecurity growth potential

Singapore's cybersecurity industry outlook

pwc

Foreword

Cybersecurity is a significant market for Singapore

Crucial to ensuring Singapore's stature as one of the world's leading financial and investment hubs, as well as the security of its strategic sectors (i.e., financial services), the role of cybersecurity is expected to become more pronounced moving forward. This is in part driven by nation-wide initiatives such as Smart Nation, and increasing digitisation of our business environment and everyday life.

Methodology

In this paper, we provide an overview of the Singapore's cybersecurity sector and its market outlook leading up to 2020 by triangulating market reports, complemented by our own market model for the city state. In addition to this secondary research, we have conducted more than 35 interviews with suppliers, customers, government agencies and international experts for their industry insights.

Our market analysis and estimates are focused on four key segments of the cybersecurity sector, namely (Figure 1):

- Identity authentication and access management
- Infrastructure protection
- Network security protection
- Security services

Figure 1: Definition of cybersecurity segments

Segments	Description	Main solutions/services included
Identity authentication access management (IAAM)	Enables the right individuals to access the right resources at the right times for the right reasons	• Web access management • Identify access management (IAM) tool
Infrastructure protection	Aims at preventing threat towards end-points, databases and cloud	• Endpoint protection • Email gateway • Web gateway • Security information and event management • Vulnerability assessment • Data loss protection
Network security protection	Ensures the protection of a network (e.g., corporate network)	• Internet service provider (ISP) equipment • Firewall • Virtual private network (VPN) • Unified threat management (UTM)
Security services	Any strategic or operational service provided to achieve higher protection against cyber threats	• Implementation • Support services • Managed security services (MSS) • Consulting services • Governance risk and compliance services (GRC) • Training

Source: Gartner

Contents

Where are we now?

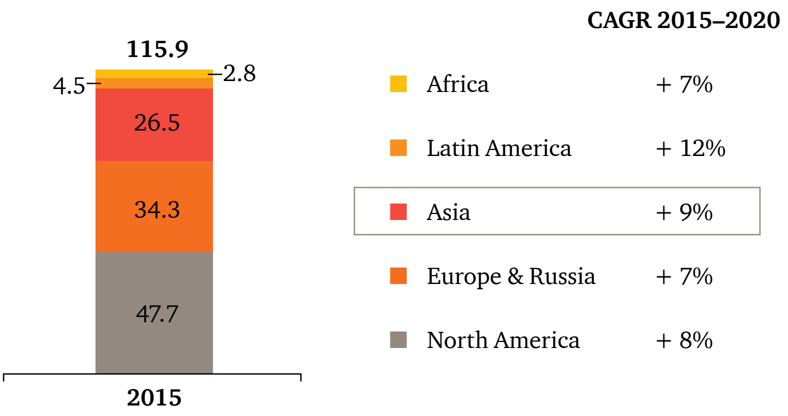
Singapore's current cybersecurity market at a glance

An expanding market

The size of the global cybersecurity market is estimated at close to S$116bn in 2015, of which Asia contributes close to 23% as the third largest region – after North America and Europe (Figure 2).

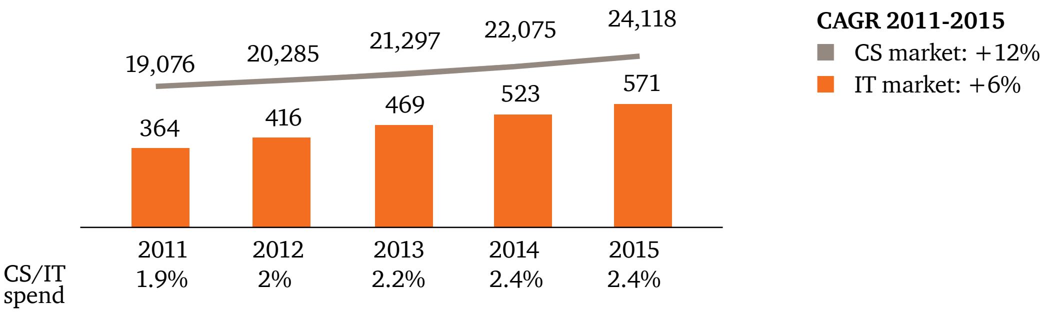
Within Asia, we assessed Singapore's cybersecurity market size to be around S$570m in the same year. While it is seemingly small in proportion to its total IT market size (at approximately 2.4%), it has seen an increase of c. 12% growth per annum over the past five years (Figure 3), making it a fast growing segment within the larger IT market.

Figure 2: Global cybersecurity market size, 2015–2020, S$bn



Source: Gartner

Figure 3: Singapore IT vs. cybersecurity market sizes, 2015, S$m

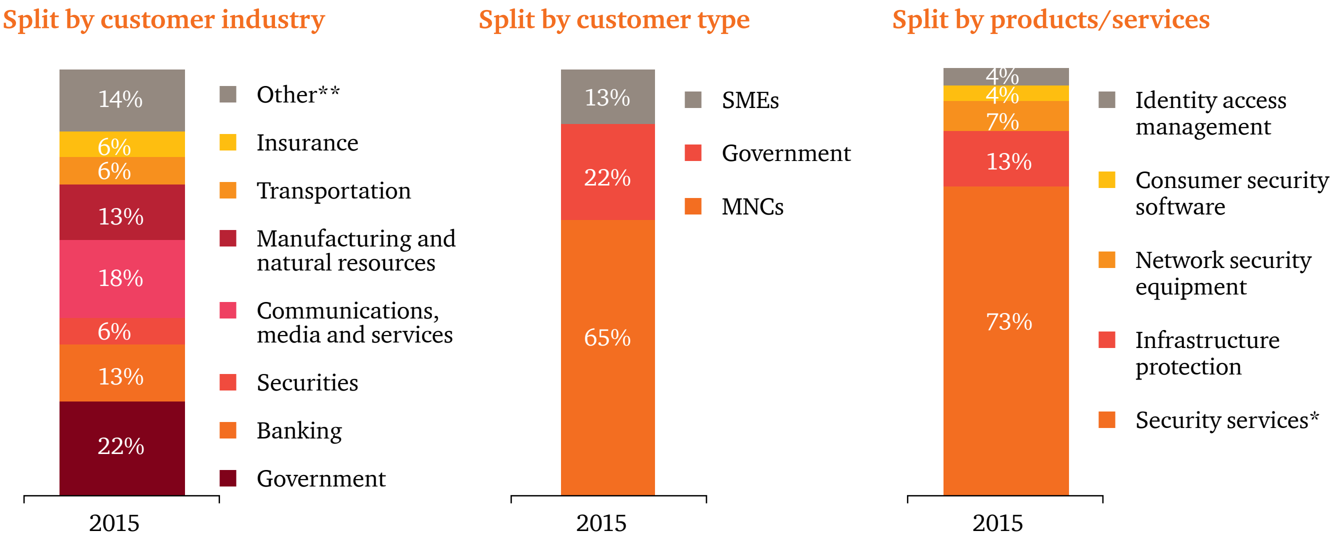


Source: Gartner, PwC Analysis, PwC Interviews

MNCs drive the largest portion of Cybersecurity spend

The government and the financial institutions make up the largest industries that invested in cybersecurity in 2015, accounting for 22% and 19% of Singapore's cybersecurity spend respectively. While small-medium-enterprises (SMEs) account for half of the city state's gross domestic product (GDP), their cybersecurity spend are much smaller compared to multinational corporations (MNCs), which drive 65% of Singapore's cybersecurity spend (Figure 4). Meanwhile, cybersecurity services account for the largest portion of Singapore's cybersecurity spend (73%) in 2015.

Figure 4: Singapore cybersecurity market size breakdown, 2015



**Security Services include implementation, IT outsourcing/MSS, consulting, and hardware support*
***Other include retail, utilities, education, healthcare providers, wholesale trade, and construction*
Note: Percentages may not always add up to 100% due to rounding
Source: Gartner, PwC Analysis, PwC Interviews

Significant growth prospects lie ahead

Future outlook of Singapore's cybersecurity sector

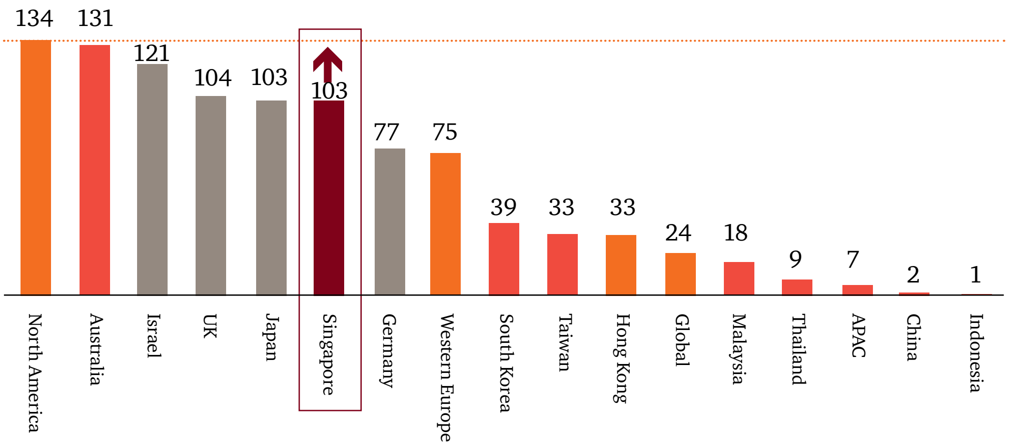
Room for growth in cybersecurity

To gauge the potential growth of Singapore's cybersecurity market, we compared the country's cybersecurity spend per capita, and cybersecurity spend as a percentage of its IT spend with the performance of its foreign counterparts.

While Singapore's cybersecurity spend per capita is higher than the other Asia Pacific economies, it is lower than that of the developed, western markets such as the US and UK (Figure 5). Despite that the city state has one of the highest IT spend per capital in the world, it allocates a lesser percentage of their IT budget to cybersecurity than its Asia Pacific contemporaries (Figure 6).

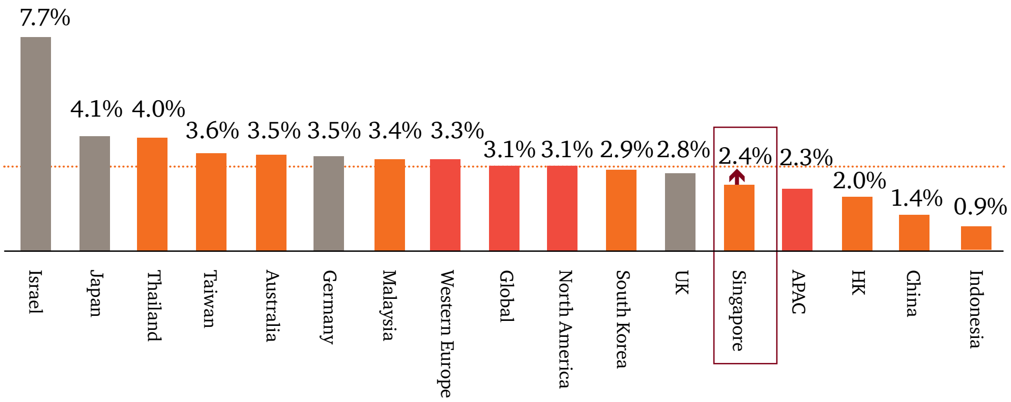
The differences between Singapore's performance and the economies leading in these two comparisons is thus indicative of the room for growth in Singapore's cybersecurity spend.

Figure 5: Cybersecurity spend per capita, 2015 S$



Source: Gartner, PwC Analysis, PwC Interviews

Figure 6: Cybersecurity spend as a percentage of IT spend, 2015



Source: Gartner, PwC Analysis, PwC Interviews

What’s driving cybersecurity demand?

The increasing frequency and sophistication of cyber threats is one of the predominant factors driving demand in cybersecurity safeguards. Other key drivers include regulatory pressure, and new technology applications, such as the internet of things (IOT) which call for another added level of cybersecurity.

Figure 7: Market demand drivers for cybersecurity in Singapore

Demand volume				Price		
Growing cyber threat	**Regulatory push**	**New usages lead to new cybersecurity needs**	**More outsourcing**	**Competitive intensity**	**Solution-commoditisation**	**New technologies**
The **amount of data stored** is exponentially growing and is increasingly seen as a prized asset Rising **frequency and sophistication** of cyber crime globally Heightened level of awareness following a number of **high profile security breaches**	Increasing scrutiny by audit committees to **protect sensitive data** Impact of **new security legislation and mandates** **Cyber insurance** is demanding stronger systems	**IOT** expands the cybersecurity field beyond traditional operations security **Increasing cloud and SAAS adoption** is creating new cybersecyrity challenges With **mobile applications and bring your own device (BYOD)** trends, endpoint segment is growing into mobile protection	**Solution complexity** - as the level of expertise required increases, in-house management of IT security becomes increasingly inefficient and more players are outsourcing it	**Increasing international and local competition** from large Software companies, global defence players, Telco operators up to niche start-ups Cybersecurity is one of the most dynamic fields for start-up funding globally	**Commoditisation -** Cost effective cloud based/ hosted services has made cybersecurity products and services more affordable **New software based technologies** are disrupting equipment market segments	**New product generations** – R&D investment is required in to generate solutions to new/complex problems which drive price premium
↗	↗	↗	↗	↘	↘	↗

Source: PwC Analysis, PwC Interviews

The biggest spenders

According to media reports, approximately 8% of the infocomm technology (ICT) budget will be set aside for cybersecurity spending (an increase from 5% previously). Coupled with the launch of Singapore's national cybersecurity strategy earlier in October 2016, the government will continue to remain a major customer/contributor to the country's cybersecurity market growth.

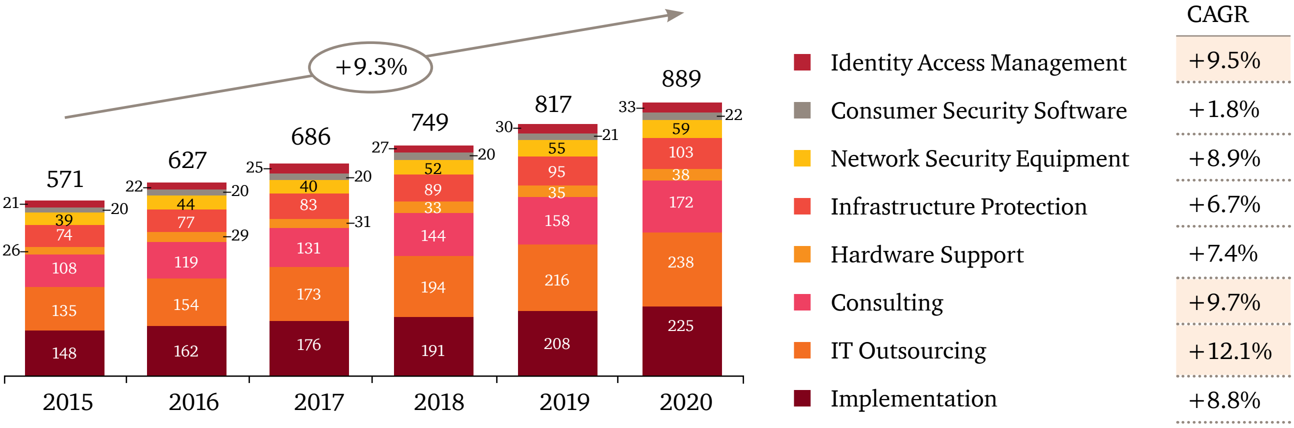
As for the private sector, SMEs are expected to be the fastest growing customer segment (+12.8% p.a. in cybersecurity spend) as the market is currently underpenetrated, and more players are building cost-effective offerings dedicated to this market. Meanwhile, MNCs will remain the largest customer segment over the long term.

Top investment priorities in cybersecurity

Singapore's cybersecurity market is expected to continue to grow at a faster pace than the broader IT market, at around 9.3% per annum over the next 5 years.
As companies are increasingly developing their cybersecurity functions, the top cybersecurity services that are expected to lead market growth are (Figure 5):

- IT outsourcing (whereby MMS is expected to lead as the main growth component)
- Cybersecurity consulting
- Identity and access management (which includes a service component in addition of hardware and software solutions)

Figure 8: Cybersecurity growth by segment in Singapore, 2015–20 (S$m)



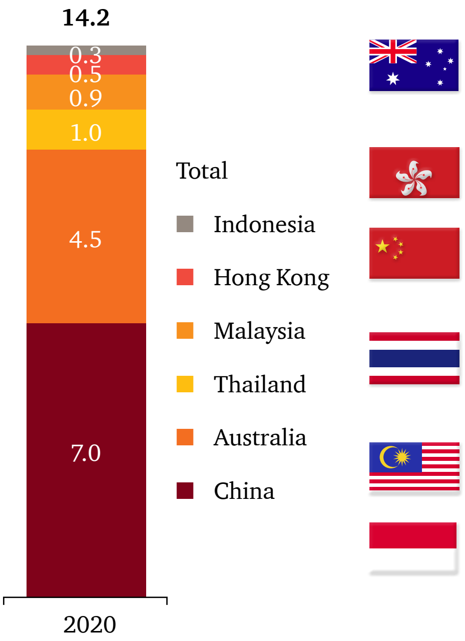
Source: Gartner, PwC Analysis, PwC Interviews

Growth opportunity beyond the border

Beyond the domestic market, local cybersecurity players may also consider further growth and export opportunities in foreign markets. The total cybersecurity market size of some of the most significant economies in the Asia Pacific region – Australia, Hong Kong, China, Thailand, Malaysia, and Indonesia – is forecasted to reach S$14.2bn by 2020 (Figure 9), of which S$6.3bn will be driven by growth in MSS, IAM and/or consulting services. Furthermore, the Middle East could be a potential export region to consider, with business prospects coming from its government sector.

However, challenges that may arise which need to be taken into consideration include data privacy issues (which can limit opportunities to handle data from Singapore), strong local competition, and protectionism.

Figure 9: Potential export market in selected APAC countries 2020, S$bn



- *Large potential market*
- *Safe business environment*
- *Strong local competition*

- *Driven by FS industry, focused on security services*
- *Nascent local competition*

- *Largest growth potential in APAC*
- *Well-developed m-Commerce*
- *Protective regulation*

- *Government legislation to support the growth of the digital economy*
- *Low local competition*

- *Some Malaysian banks already using MSS services from Singapore*

- *Strong growth potential in e-Commerce and the digital economy*
- *Lowest CS spend in APAC*
- *Difficult business environment*

Source: Gartner, PwC Analysis

The talent challenge

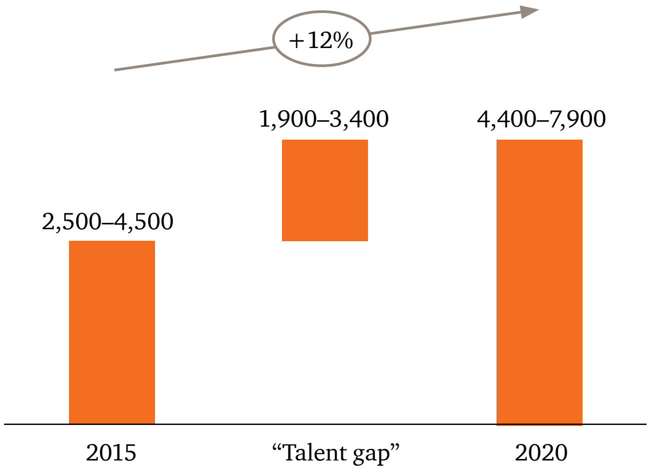
Cybersecurity sector's top impediment in meeting rising demands

Based on our in-depth interviews with Singapore cybersecurity players, we observe that talent is one of their biggest growth constraints. This issue is not specific to Singapore only as the industry faces a shortage of talent at a global level.

The talent gap, estimated at between 1,900 and 3,400 people, will need to be filled in order to support the projected growth (in both domestic and export markets) of Singapore's cybersecurity sector over the next five years (Figure 10). The shortage is especially acute for experienced professionals in the following areas (Figure 11):

- Threat and vulnerability assessment
- Incident and crisis management
- Security management

Figure 10: Estimated number of cybersecurity full-time employees in Singapore to support the growth of the domestic and export markets*, 2015–2020



**Estimation based on forecasted market growth rate assuming Singapore will grow as an export base on top of its domestic spend growth*
Source: PwC Analysis

Figure 11: Cybersecurity roles in demand

↗ Average market growth   ↑ Above average market growth   → Below average market growth

	Security management	Security audit	Security operations	Threat and vulnerability management	Incident and crisis management	Engineering and architecture	R&D
Description	• Risk management • Governance • Compliance	• Information sytem audit (internal and external)	• Security operations centre (SOC) operators • Security administration	• Threat intelligence • Data analysis • Penetration testing	• Incidence response • Forensics • Malware analysis	• Integration engineering • Software development and architecture	• Researcher • Development engineering
Forecast growth (2015–20)	↑	↗	→	↑	↑	→	↑
Positions in demand	• Chief Information Security Officer (CISO) • Technology risk manager • Information security officer	• Overall supply seems adequate	• SOC analyst/ manager	• Threat intelligence analyst/ manager • Data analyst/ scientist • Senior penetration tester • System security configuration analyst/ manager	• Forensic analyst/ manager • Malware analyst/ manager • Security incident response analyst/ manager • Penetration tester	• Security architect • Security software development manager • Lead security engineer	• Principal investigator • Principal researcher • Principal engineer
Talent gap evaluation	• Demand is triggered by increased awareness & regulatory constraint • Mid-level information security officers with business acumen and operational expertise are highly sought after • Adequate supply of talent in audit		• Adequate supply of junior SOC analysts to meet most market demands • Demand for security threats and vulnerability management positions is mainly driven by the financial services sector • Senior positions in incident & crisis management and threat & vulnerability management are hard to fill as these are emerging fields with a limited talent pool			• Lower-tier security engineers are relatively easy to find • Security engineers need to be groomed to meet the growing demand for security architects • R&D talent will be needed in emerging fields like data analytics and threat intelligence	

**Excludes sales, marketing, and sales, general and administration (SG&A)*

While tertiary education institutions have started to help fill the talent gap by launching cybersecurity specific degrees/qualifications, ongoing talent issues remain. Some of the key talents issues businesses will need to keep in mind include (Figure 12):

- How to attract and retain cybersecurity and information and communications technology (ICT) talent?
- How to develop talent, both vertically (e.g., deep technical expertise) and horizontally (e.g., extensive business and management acumen)?

Figure 12: Cybersecurity manpower issues

		Interview responses from cybersecurity players
Attract talent	Short-term	*"Slow influx of fresh graduates to meet the growing short-term needs"* *"Talent shortage leading to Inflationary pressure on salaries"* *"Start-ups more at risk of being impacted by talent shortage as they don't have the established brands nor the clear career tracks"*
	Long-term	*"ICT jobs as a whole are seen as less attractive than other sectors like financial services making it difficult to attract talent especially for the more technical positions"*
Develop talent	Vertical skills	*"Fresh cybersecurity graduates are lacking deep practical experience and private companies have to build in-house academies "* *"Lack of scale and global talent in R&D"*
	Horizontal skills	*"Skill gap especially strong for local senior positions where business acumen and strategic thinking are required on top the technical skills"*

Moving forward

Strategic 'next steps' to further develop Singapore's cybersecurity sector

A lot is currently being done to develop Singapore's cybersecurity ecosystem, with efforts coming from both the public (i.e. government and its agencies) and private sectors.

Given Singapore's clear and strong regulatory framework – one that is more mature than most of its Asia Pacific counterparts – coupled with strong demand drivers in its domestic market, and national initiatives such as Smart Nation, its cybersecurity industry has the advantageous climate to grow strongly.

Significant development could be achieved in two areas in order for Singapore players to make the most of the local cybersecurity ecosystem. Firstly, cybersecurity players need to strengthen their local expertise in core areas such as MSS, IAAM and cybersecurity consulting to develop next product generations and export these competencies abroad. Secondly, they could build a differentiated positioning around niche products benefiting from Singapore context (e.g. financial services, critical infrastructure, Smart Nation/ Cities) (Figure 13).

Meanwhile the government has a key role to play in stimulating the SME market, in addition to stepping up its cybersecurity spend and measures for its strategic clusters (e.g., government and financial services). Furthermore, it is an imperative to increase collaborations/partnerships between the private and public sectors to accelerate development and achieve inclusive growth (Figure 14).

Figure 13: Opportunities in cybersecurity for Singapore

Key opportunities			
Catch up	Build		Win
Level up cybersecurity protection and spend for sensitive industry clusters (e.g., the government sector, financial services and more)	**Build on local expertise to expand overseas**	**Advanced MSS** (New generation SOCs)	**Predictive analytics, threat intelligence**
		Advanced IAAM (Multi-factor authentication, IAM)	**Security as a service, cloud**
		Advanced Consulting (GRC, forensics)	**Pro-active risk management, smart forensics**
Develop the SME market Increasing awareness and leveraging cost-effective solutions (e.g., cloud)	**Build a differentiated positioning around niche products**	**Financial services**	**Mobile banking solutions**
		Critical infrastructure	**Integrated electronic and cybersecurity**
		Smart Nation	**IOT**

Figure 14: Areas for collaboration in cybersecurity

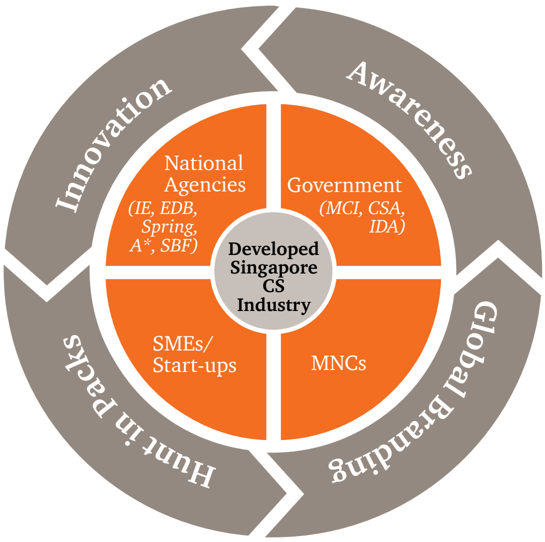
Potential areas for collaboration

Awareness
Raise cybersecurity awareness, with a special focus on SMEs

Innovation
Strengthen R&D and innovation capabilities

Global Branding
Leverage Singapore "trust" brand and grow it globally for cybersecurity

Hunt in Packs
Coordinate and combine sales efforts on the export market around national priorities such as Smart Nation/cities


Innovation
Awareness
Global Branding
Hunt in Packs
National Agencies (IE, EDB, Spring, A*, SBF)
Government (MCI, CSA, IDA)
Developed Singapore CS Industry
SMEs/ Start-ups
MNCs

Connect with us

Richard Skinner
Strategy Leader
PwC Singapore
richard.skinner@sg.pwc.com

Dimitri Le Bert
Director, Strategy
PwC Singapore
dimitri.le.bert.@sg.pwc.com

Oliver Wilkinson
Managing Director, Strategy
PwC Singapore
oliver.wilkinson@sg.pwc.com

Gael Andry
Manager, Strategy
PwC Singapore
gael.m.andry@sg.pwc.com

About PwC PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details. “PricewaterhouseCoopers” refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity. In the context of this report, unless otherwise indicated, “PricewaterhouseCoopers LLP” or “PwC” refers to the Singapore entity operating as PricewaterhouseCoopers LLP.

Disclaimer This report has been prepared using information provided to PricewaterhouseCoopers LLP and available at the time of preparation of this report. PricewaterhouseCoopers LLP does not accept any responsibility for any reliance placed on this report by any person and hereby disclaims any liability for any loss or damage caused by errors or omissions, whether such errors or omissions resulted from negligence, accident or other causes. PricewaterhouseCoopers LLP makes no representations about the analysis or data included in this report. PricewaterhouseCoopers LLP has received a fee for the preparation of this report and takes responsibility for the independence of the research and independence of the analysis contained in this report. Please notify PricewaterhouseCoopers LLP of any errors or omissions identified in this report.