SINGAPORE'S CYBERSECURITY STRATEGY

Singapore's Cybersecurity Strategy

ISBN: 978-981110812-9

Cyber Security Agency of Singapore
www.csa.gov.sg

Design and layout by:
APT811 Design & Innovation Agency
www.apt811.com

PRIME MINISTER'S FOREWORD

Singapore is an international centre of exchange and commerce. We must always be open to new technologies and know-how, in order to connect ideas, economies and cultures across the world.

Digitally, Singapore is one of the most connected nations in the world. We have long embraced infocomm technologies for economic and social development. Today, we have more phone lines than people. Almost all households have high-speed broadband Internet access.

However, reliance on infocomm technologies also makes us vulnerable. Cyber threats and attacks are becoming more sophisticated, with more severe consequences. We cannot take cybersecurity for granted.

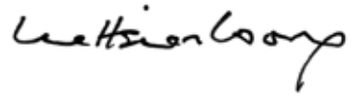
The Cybersecurity Strategy outlines Singapore's vision, goals and priorities. We are determined to protect essential services from cyber threats, and to create a secure cyberspace for businesses and communities. The Cyber Security Agency of Singapore will take the lead, and work with other agencies and private sector partners to achieve this.

The Government cannot do it alone. Businesses are responsible for protecting customers' personal data. Individuals need to practise good cyber hygiene to keep personal devices and data safe. If we each do our part to use our systems and devices responsibly, then collectively we can help to protect Singapore's cyberspace.

Cyber attackers do not respect jurisdictions. All countries, especially highly-connected ones like Singapore, benefit from international cooperation in securing global infocomm infrastructures and responding to cyber threats. Singapore will work closely with other countries to build consensus in cyber norms, strengthen capacity and address cyber threats and crimes.

As an industry, cybersecurity offers opportunities and good jobs for Singaporeans. The Government will provide education and training opportunities for Singaporeans who wish to pursue a career in cybersecurity.

Together, we will build a resilient and trusted cyber environment for Singapore – one that harnesses the benefits of technology to improve the lives of Singaporeans.



Lee Hsien Loong

CONTENTS

SINGAPORE'S CYBERSECURITY STRATEGY AT A GLANCE 4

INTRODUCTION 6

1 A RESILIENT INFRASTRUCTURE 8

Protect Our Essential Services 12

Respond Decisively to Cyber Threats 16

Strengthen Governance and Legislative Framework 19

Secure Government Networks 20

2 A SAFER CYBERSPACE 22

Combat Cybercrime 26

Enhance Singapore's Standing as a Trusted Hub 30

Promote Collective Responsibility 32

3 A VIBRANT CYBERSECURITY ECOSYSTEM 34

Establish a Professional Cybersecurity Workforce 36

Extend Singapore's Cybersecurity Advantage 38

Innovate to Accelerate 40

4 STRONG INTERNATIONAL PARTNERSHIPS 42

Forge International and ASEAN Cooperation to Counter Cyber Threats and Cybercrime 44

Champion International and ASEAN Cyber Capacity Building Initiatives 46

Facilitate International and Regional Exchanges on Cyber Norms and Legislation 47

SINGAPORE'S CYBERSECURITY STRATEGY AT A GLANCE

Singapore's Cybersecurity Strategy aims to create a resilient and trusted cyber environment. This will enable us to realise the benefits of technology and so secure a better future for Singaporeans.

Four pillars underpin our strategy. We will **strengthen the resilience of Critical Information Infrastructures** (CIIs). We will mobilise businesses and the community to **make cyberspace safer**, by countering cyber threats, combating cybercrime and protecting personal data.

We will **develop a vibrant cybersecurity ecosystem** comprising a skilled workforce, technologically-advanced companies and strong research collaborations, so that it can support Singapore's cybersecurity needs and be a source of new economic growth. Finally, given that cyber threats do not respect sovereign boundaries, we will step up efforts to **forge strong international partnerships**.

> "Cybersecurity is a team effort, everyone has a part to play, and everyone has to play their part. The Government will take the lead to spearhead initiatives to enhance Singapore's cybersecurity stance, and we will need everyone's cooperation to reap long term benefits for the cyber ecosystem. We aim to build a Smart Nation – one that will be enabled by trustworthy infrastructure and technology."
>
> **Minister-in-charge of Cybersecurity, Dr Yaacob Ibrahim,**
> GovernmentWare 2015

Building a Resilient Infrastructure

OUR STRATEGY:

To secure our digitally-enabled economy and society, the Government will work with key stakeholders – private sector operators and the cybersecurity community – to strengthen the resilience of our CIIs.

First, we will enhance our CII Protection Programme to establish robust and systematic cyber risk management processes across all critical sectors. Second, we will improve our sectors' response and recovery plans to breaches. We will mount multi-sector cybersecurity exercises to test cooperation across multiple sectors and address inter-dependencies during major cyber-attacks. We will also expand and beef up national resources such as the National Cyber Incident Response Team (NCIRT) and the National Cyber Security Centre (NCSC). Next, we will introduce the Cybersecurity Act to give the Cyber Security Agency of Singapore (CSA) greater powers to secure our CIIs. Finally, as threats to government networks will continue to grow, we will expand efforts to secure government systems and networks, so as to protect citizens' and official data.

Creating a Safer Cyberspace

OUR STRATEGY:

Cyber technology can enable and empower business and society, but only if it is safe and trustworthy. A safer cyberspace is the collective responsibility of the Government, businesses, individuals and the community.

First, to effectively deal with the threat of cybercrime, the Government will implement the recently launched National Cybercrime Action Plan. Second, we will enhance Singapore's standing as a trusted hub by fostering a trusted data ecosystem. We will work with global institutions, other governments, industry partners and Internet Service Providers to quickly identify and reduce malicious traffic on our Internet infrastructure. Finally, communities and business associations can play their part by fostering their members' understanding of cybersecurity issues and promoting the adoption of good practices.

Developing a Vibrant Cybersecurity Ecosystem

OUR STRATEGY:

Cybersecurity is both an imperative and an opportunity. With advanced infrastructure and a highly-skilled IT workforce, Singapore is well-positioned to build a vibrant cybersecurity ecosystem.

First, the Government will collaborate with industry partners and Institutes of Higher Learning (IHLs) to grow the cybersecurity workforce, including encouraging existing cybersecurity professionals to deepen their skills. Second, we will develop strong companies and nurture local start-ups to ensure that best-in-class solutions are available locally. There are also opportunities for cybersecurity companies to leverage Singapore's traditional strengths in areas such as financial and infocomm services to develop exportable solutions. Third, we will foster closer partnerships between academia and industry so as to harness cybersecurity R&D in a more targeted manner to deliver effective solutions. With skilled professionals, technologically-advanced companies and strong research collaborations, Singapore can be at the global forefront of cybersecurity innovation and create economic opportunities for Singaporeans and the industry.

Strengthening International Partnerships

OUR STRATEGY:

Cybersecurity is a global issue. Cyber threats do not respect sovereign boundaries; indeed, jurisdictional gaps are exploited to the cyber-attacker's advantage. Cyber-attacks disrupting one country can have serious spill-over effects on other countries as our inter-dependencies have increased through trade and global financial markets.

Singapore is committed to strong international collaboration in cybersecurity for our collective global security. Singapore will actively cooperate with the international community, particularly ASEAN, to address transnational cybersecurity and cybercrime issues. We will champion cyber capacity building initiatives, and facilitate exchanges on cyber norms and legislation. Through international consensus, agreement, and cooperation, we can make cyberspace a safer and more secure place for all.

INTRODUCTION

"Cybersecurity is important for Singapore given our high dependence on information technology and the Internet, and cybercrime is also growing. Cyber-attacks can take many forms and come from many sources. They range from defacements of website and data theft, often by persons who hide behind the anonymity of cyberspace [and] can also include systemic threats"

Deputy Prime Minister Teo Chee Hean,
Committee of Supply, 6 Mar 2013

Cyber-attacks are increasingly frequent, sophisticated and impactful. Globally, we have seen a surge in the number of cyber incidents, such as ransomware, cyber theft, banking fraud, cyber espionage and disruptions to Internet services. Attacks on systems that run utility plants, transportation networks, hospitals and other essential services are more frequent. Successful attacks result in disruptions which could cripple economies, and lead to loss of life.

The advent of the Internet of Things will further increase the attack surface. Left unchecked, malicious entities can find more ways to launch attacks, steal data and make cyberspace dangerous for all. The result is a cyberspace that is hostile, and where basic interactions and transactions cannot be trusted.

Singapore has consistently taken cyber threats seriously and developed timely responses. Our cybersecurity journey started a decade ago with the first Infocomm Security Masterplan in 2005. The Masterplan was a coordinated effort to secure Singapore's digital environment and strengthen public sector cybersecurity capabilities. Since then, Singapore's cybersecurity capabilities have grown. With the formation of the Singapore Infocomm Technology Security Authority (SITSA) in 2009, we developed the capability to coordinate national-level responses against large-scale cyber-attacks, particularly against our critical information infrastructures.

In 2015, the Cyber Security Agency of Singapore (CSA) was formed as the central agency to oversee and coordinate all aspects of cybersecurity for the nation. CSA is empowered to develop and enforce cybersecurity regulations, policies, and practices.

While much has been achieved so far, the threats have also become more sophisticated. We are even more dependent on digital technology, especially as we develop a Smart Nation of digitally-enabled businesses and lives. Cybersecurity, beyond a necessity to defend and protect, is also an enabler for our future economy and society.

This Strategy is a statement of Singapore's vision and priorities for cybersecurity. It aims to catalyse participation by all stakeholders - government agencies, the cyber industry, professionals and students, academia and researchers, and providers of essential services. Together, we will ensure the resilience of our national infrastructure and a safer cyberspace, supported by a vibrant ecosystem that provides good jobs and economic opportunities for Singaporeans. It also signals Singapore's willingness to forge strong partnerships with the international community to combat the transnational nature of cyber threats.

Our Smart Nation Journey

Singapore is transforming to become a Smart Nation, where Singaporeans are empowered by technology to lead meaningful and fulfilling lives, where digital connectivity leads to stronger community bonds, and where the power of networks, data and infocomm technologies is harnessed to create economic opportunities.

Smart Nation is a whole-of-nation rallying call for citizens, companies, and government agencies to work hand-in-hand to seize the many possibilities of digital technology. We are putting in place the necessary infrastructure and policies to build capabilities, and to create a conducive ecosystem where people and companies co-create innovative solutions to enhance the lives of our citizens.

OUR CYBERSECURITY JOURNEY SO FAR

2005 Infocomm Security Masterplan (ISMP) (2005-2007)
The Info-communications Development Authority (IDA) launched Singapore's first Infocomm Security Masterplan to coordinate cybersecurity efforts across the Government. A key priority was building basic capabilities within the public sector to mitigate and respond to cyber threats.

2008 Infocomm Security Masterplan (2008-2012)
The second Masterplan focused especially on the security of Singapore's CIIs, with a vision of making Singapore a 'Secure and Trusted Hub'.

2009 Singapore Infocomm Technology Security Authority (SITSA)
SITSA was established under the Ministry of Home Affairs (MHA) to safeguard Singapore against cyber-attacks and cyber-espionage. SITSA's responsibilities as a national specialist authority included overseeing the preparation and securing of CIIs against cyber threats.

2013 National Cyber Security Masterplan (NCSM2018)
The third Masterplan expanded to cover the wider infocomm ecosystem, which includes businesses and individuals, in addition to the previous focus on CIIs. It sought to make Singapore a 'Trusted and Robust Infocomm Hub'.

2013 National Cybersecurity R&D (NCR) Programme
The National Cybersecurity R&D Programme was established in October 2013 to develop R&D expertise and capabilities in cybersecurity for Singapore. It aims to improve the trustworthiness of cyber infrastructure, with emphasis on security, reliability, resilience and usability. It is now co-managed by the National Research Foundation and the Cyber Security Agency of Singapore.

2014 National Cyber Security Centre (NCSC)
The NCSC was formed as part of SITSA, to maintain cyber situational awareness, correlate cybersecurity events across sectors, and coordinate with the respective lead agencies to provide a national-level response to large-scale, cross-sector cyber incidents.

2015 Cyber Security Agency of Singapore (CSA)
CSA was established under the Prime Minister's Office (PMO) and is managed administratively by the Ministry of Communications and Information (MCI). With its formation, all agencies and initiatives related to cybersecurity – the Singapore Computer Emergency Response Team (SingCERT), national cybersecurity master-planning and development functions from IDA, and SITSA – were brought under a single agency.

CSA is dedicated to the development of cybersecurity, protection of CIIs and essential services, and coordination of national efforts against large-scale cyber incidents. CSA is also empowered to develop and enforce cybersecurity regulations, policies, and practices. It will coordinate efforts across government, industry, academia, businesses and the people sector, as well as internationally.

2015 Cybercrime Command
The Ministry of Home Affairs (MHA) established the Cybercrime Command as a unit within the Criminal Investigation Department (CID) of the Singapore Police Force (SPF). The Command works closely with other law enforcement agencies and industry stakeholders, including the INTERPOL Global Complex for Innovation (IGCI) located in Singapore, to investigate cybercrimes.

2016 National Cybercrime Action Plan (NCAP)
The NCAP was launched by the Ministry of Home Affairs (MHA) in July 2016. The plan spells out the priorities needed in the fight against cybercrime. These include a) the need for public education on staying safe in cyberspace; b) the development of capabilities to fight cybercrime; c) strengthening cybercrime laws; and d) building local and international partnerships.

CHAPTER 1

A RESILIENT INFRASTRUCTURE

Behind the scenes, in every city (and Singapore is no exception), a gamut of essential services and infrastructure are needed to keep a modern metropolis running smoothly. Essential services such as energy, banking, healthcare and transport are powered by infocomm technology. Cyber-attacks on these Critical Information Infrastructures (CIIs) can interfere with these essential services. At best, they lead to inconveniences. At worst, they can result in significant disruptions to the economy and to our society.

The effects of a cyber-attack on Singapore have ramifications beyond our shores. Singapore is an open economy and connected to the rest of the world. It is a major international centre for trade, finance and logistics. A cyber-attack on Singapore could potentially impact the wider regional and global economy.

Singapore has to ensure that its CIIs are not just resilient against physical threats, but also against cyber threats. A cyber-resilient infrastructure will provide peace of mind to Singaporeans. A cyber-resilient infrastructure will reinforce confidence in Singapore as a resilient and trusted global centre of trade and commerce.

The Government will work with key stakeholders - the CII operators and the cybersecurity community - in four major areas.

We will:

Step up the protection of our essential services. We will implement a **CII Protection Programme** which emphasises robust and systematic cyber risk management processes, and the importance of a culture of cyber risk awareness across all levels of CII organisations. We will increase the adoption of **Security-by-Design** practices to address cybersecurity issues upstream and along the supply chain.

Enhance our capability to respond decisively to cyber threats. We will enhance our **national cyber situational awareness** and conduct regular multi-sector cybersecurity exercises with more complex scenarios and involving more and more sectors. We will build up **more National Cyber Incident Response Teams (NCIRT)** and **enhance the Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP)** of the critical sectors.

Strengthen our cybersecurity governance and legislative framework. We will introduce a **new Cybersecurity Act** that will require CII owners and operators to take responsibility for securing their systems and networks. The Act will also facilitate the sharing of cybersecurity information with and by CSA, and empower CSA and sector regulators to work closely with affected parties to resolve cybersecurity incidents in a timely manner.

Make Government systems more secure. The Government will expand its efforts to secure its systems and networks. This includes allocating **8 per cent of the total Government ICT expenditure to cybersecurity**. We will also **reduce the attack surface** of Government systems, **enhance cyber situational awareness** in the government sector and **sharpen cyber incident management**.

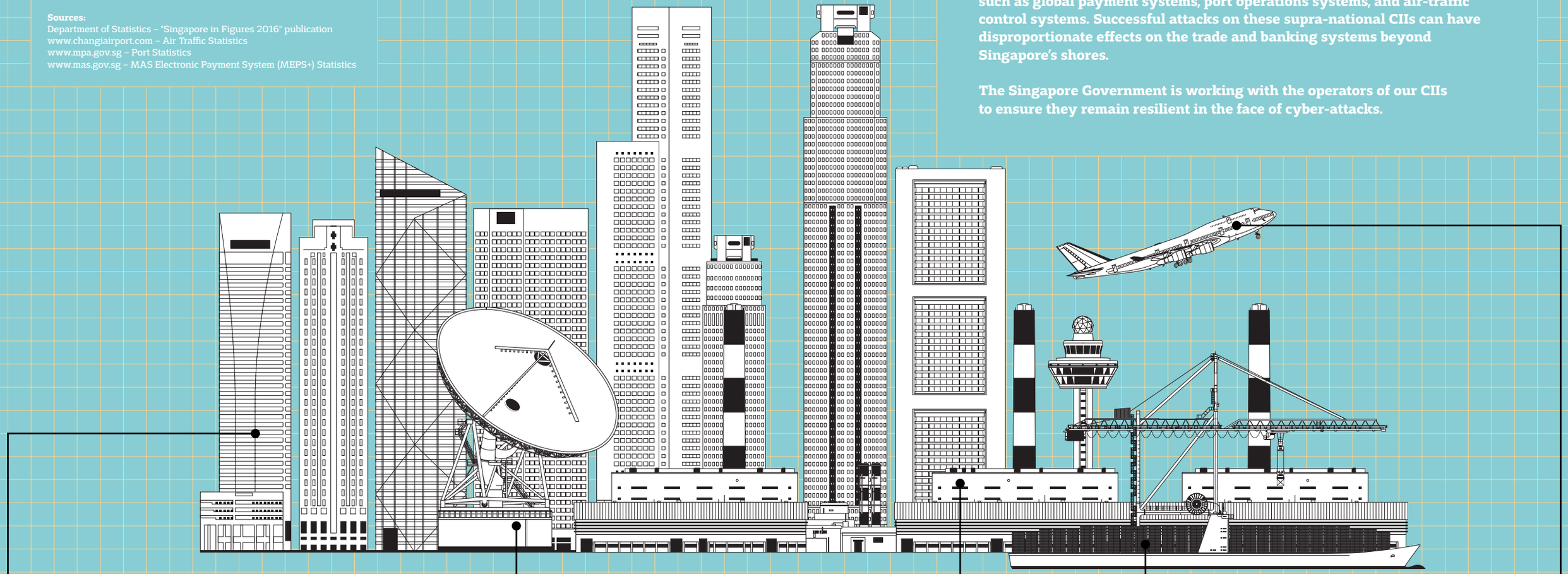
SINGAPORE'S CRITICAL INFORMATION INFRASTRUCTURE SECTORS

Sources:
Department of Statistics – "Singapore in Figures 2016" publication
www.changiairport.com – Air Traffic Statistics
www.mpa.gov.sg – Port Statistics
www.mas.gov.sg – MAS Electronic Payment System (MEPS+) Statistics

The reliable supply of essential services depends on the security of the computer and network infrastructure in Singapore's Critical Information Infrastructure (CII) sectors. Today, we have identified 11 CII sectors, which cut across utilities, transport, and services.

Cyber-attacks on Singapore's CIIs may have spill-over effects regionally and globally. As an international financial, shipping and aviation hub, Singapore also houses critical systems that transcend national borders, such as global payment systems, port operations systems, and air-traffic control systems. Successful attacks on these supra-national CIIs can have disproportionate effects on the trade and banking systems beyond Singapore's shores.

The Singapore Government is working with the operators of our CIIs to ensure they remain resilient in the face of cyber-attacks.



SERVICES

Singapore is a major financial centre that processes massive amounts of transactions every second. For example, our local inter-bank payment systems handle millions of transactions totalling trillions of dollars annually. Many of our public services – government transactions, healthcare, emergency services – are increasingly reliant on complex underlying computer systems to serve millions of users each year. The Government Technology Agency (GovTech), Ministry of Home Affairs (MHA), MOH Holdings (the holding company of Singapore's public healthcare entities), Info-communications Media Development Authority (IMDA) and the Monetary Authority of Singapore (MAS) are committed to strengthening the cybersecurity of the systems delivering government and emergency services, healthcare, media, and banking and financial services.

UTILITIES

Power, water and telecommunications are the lifeline of modern cities. In particular, the failure of power and telecommunications services can bring other services to a grinding halt. The Energy Market Authority (EMA), Public Utilities Board (PUB) and Info-communications Media Development Authority (IMDA) will work closely with the private operators delivering these services to raise their cybersecurity posture and ensure the reliability of these services.

TRANSPORT

Singapore is an international logistics hub. The Singapore Port and Changi Airport are among the world's busiest. The Port is a major transhipment hub that handles more than 130,000 vessels and 30 million containers each year. The Airport sees more than 340,000 flights, 55 million travellers, and 1.8 million tons of cargo annually. Our public transport system handles 7.5 million passenger trips per day. The Land Transport Authority (LTA), Maritime and Port Authority (MPA) and Civil Aviation Authority of Singapore (CAAS) have put in place governance frameworks and are building cybersecurity capability to ensure that our transport and logistics systems are robust.

PROTECT OUR ESSENTIAL SERVICES

Operators increasingly rely on computer networks and the Internet to maintain essential services and to serve their businesses and consumers. For CII operators, the gain in efficiency and productivity is significant – but so are the increased vulnerabilities of essential services to cyber disruption.

To ensure the continuous delivery of essential services, CII operators need both physical resilience and cyber resilience. Cyber resilience is the ability of our CIIs to withstand cyber-attacks, allowing them to continue operating under the toughest conditions and recover quickly after a disruption. We must raise the cyber resilience of our essential services, and we can achieve this only with the trust and participation of all stakeholders – the Government, CII operators, and the cybersecurity community.

Singapore will:

- **Implement across all critical sectors, a CII Protection Programme with robust and systematic cyber risk management processes. A key part of the CII Protection Programme is to grow a culture of cyber risk awareness across all levels of a CII organisation. From the CEO to the employee, cybersecurity must be seen as a business concern and not just one for the IT department.**

- **Pre-empt cyber vulnerabilities by going upstream and promoting Security-by-Design practices. Cybersecurity will no longer be an afterthought, but will be consciously implemented throughout the lifecycle of technology systems.**

Implement CII Protection Programme

The Government will roll out a holistic CII Protection Programme for government agencies and CII operators. It will build on the Cybersecurity Readiness Maturity Assessment programme implemented in 2012, which has enabled agencies and operators identify areas for improvement.

The CII Protection Programme will, firstly, establish the foundation to facilitate information exchange among CII operators through clear policies and guidelines. Second, it will enable targeted and systematic improvements through clearer measurements of governance maturity and networks' cybersecurity hygiene. Third, it will require operators to foster a culture of cyber-risks literacy across all levels in organisations, proactively address cyber-risks and ensure that their practices are consistent with policies. With a deep understanding of cyber risks, sectors take ownership and provide management focus to implement effective CII protection plans that are tailored to the unique circumstances of each sector.

The goal is for all critical sectors to establish robust and systematic cyber risk management processes and capabilities that are effective against the evolving cyber threats.

Systematic Cyber Risk Management

A systematic cyber risk management framework comprises:

1. thorough identification and prioritisation of cyber risks and CIIs through risk assessments, vulnerability assessments and system reviews;
2. well-informed and conscious trade-offs in security, cost and functionality, decided at management levels of appropriate seniority;
3. sound systems and procedures to mitigate and manage these risks, including disaster recovery and business continuity plans;
4. effective implementation that encompasses awareness building and training across the organisation; and
5. continuous measurement of performance through process audits and cybersecurity exercises.

Cybersecurity Maturity Assessment

The Government has been using the Readiness Maturity Index (RMI) framework to assess the readiness of CII sectors in terms of their capabilities for risk-based mitigation, early detection of threats, and robustness of the response measures. The RMI is the metaphorical health check that directs the CII sectors' effort to manage cyber risks, and facilitates the development of action plans to improve governance and procedures.

Promote Security-by-Design

Security-by-Design is an approach in the system development lifecycle process to ensure that our applications and systems are built, deployed, maintained, upgraded and disposed of securely.

The Government will promote the adoption of Security-by-Design in several ways:

- Progressively institutionalise Security-by-Design into the governance framework for CII protection;
- Promote the practice of penetration testing to discover vulnerabilities early for remediation at the design stage;
- Build a strong community of practice in product and system testing based on established international standards, such as the Common Criteria product assurance certification; and
- Continue to refine methodologies and develop new security validation tools to improve the efficacy of Security-by-Design.

Opening of the CREST Examination Facility for Penetration Testing Certifications and Accreditations at the Singapore Institute of Technology

The implementation of Security-by-Design has to be complemented with highly skilled professionals who can carry out security validation processes rigorously and proficiently. The introduction of CREST penetration testing certifications and accreditations in Singapore is one means of raising the professional competency standards.

Why is Security-by-Design important?

Security-by-design is a best practice to ensure that system is developed with security consideration upfront and throughout its lifecycle. By integrating risk assessment into the system development lifecycle, trade-offs between security, cost and functionality are deliberated. The trade-off decisions should be made by well-informed management at the appropriate level of decision making. This ensures that the system is optimised for the conditions in which it is to be used.

Subscribing to Security-by-Design will reduce piecemeal implementation and the need for costly and often ineffective retrofitting. Cybersecurity, when thoughtfully considered and incorporated at the design stage of a system will result in an organically robust system design that can better withstand cyber threats.

“The first priority on our journey towards a Smart Financial Centre is therefore to continually strengthen the industry’s cybersecurity.”

Mr Ravi Menon,
Managing Director, Monetary Authority of Singapore (MAS),
Global Technology Law Conference,
June 2015

Designing cybersecurity into FinTech

The Monetary Authority of Singapore (MAS) has formed a Financial Technology & Innovation Group since August 2015 to drive the Smart Financial Centre initiatives. This Group is responsible for formulating regulatory policies and developing strategies to facilitate the use of technology and innovation to enhance efficiency and better manage risks in the financial sector. Efforts by MAS to manage risks associated with FinTech include:

1. Establishing a FinTech Innovation Lab that allows stakeholders to experiment with FinTech solutions, including security solutions;
2. Establishing “regulatory sandboxes” that can be used to carve out a safe and conducive space to experiment with FinTech solutions, and where the consequences of failure can be contained; and
3. Providing financial support through the Financial Sector Technology & Innovation scheme for projects that uplift the cybersecurity ecosystem in Singapore.

RESPOND DECISIVELY TO CYBER THREATS

An effective cyber defence must assume that there can and will be successful cyber-attacks. When such attacks materialise, the cyber defenders must be able to mount a robust response and implement reliable recovery plans. This can only be possible with a comprehensive framework for preparedness.

Singapore has developed a national cybersecurity response plan which allows for timely response and ground initiative at the local level, complemented with effective coordination and strategic support at the sectoral and national level. The plan envisages three tiers of response – Tier 1 for cyber campaigns that threaten national security, Tier 2 for cyber-attacks on a sector, and Tier 3 for cyber-attacks on a specific operator. The plan requires CSA to work closely with CII operators and the cybersecurity community to ensure an effective response.

The national response to a cyber-attack will be led by an inter-agency Cybersecurity Crisis Management Group, or CMG (Cyber). It is led by the Permanent Secretary of the Ministry of Communications & Information, supported by CSA, and comprises senior policy decision-makers from government agencies overseeing the different critical sectors. CMG (Cyber) serves dual functions: (a) it is responsible for the development of cybersecurity policies and standards, and oversees the implementation of cybersecurity protection measures in the critical sectors; and (b) in a cyber crisis, it mobilises the necessary resources and directs the operational responses to provide a coordinated response to the threat.

Integration of Threat Discovery, Analysis and Incident Response

The National Cyber Security Centre (NCSC) monitors and analyses the cyber threat landscape to maintain cyber situational awareness and anticipate future threats. In the event of large-scale cyber incidents involving multiple sectors, NCSC coordinates with the sector regulators to provide a national level response and facilitate quick alerts to cross-sector threats.

The Government is investing in technologies and systems that will strengthen and integrate the NCSC's three key functions of threat discovery, threat analysis and incident response. This will enable faster threat discovery and operational response for cross-sector cyber incidents.

More Comprehensive Cybersecurity Exercises

Cybersecurity exercises are important ways to raise the readiness of sectors, build incident response plans and capabilities, and improve communication and coordination between the CII operators and government agencies. The Government will conduct these cybersecurity exercises at both the sector and national levels.

Sector exercises will run with more complex scenarios and more sophisticated attack methods. This will enhance the capability of the sectoral cyber response teams and the quality of incident management by the C-suite decision-makers in the CII operators.

National-level exercises will encompass more and more sectors, with an emphasis on the inter-dependent nature of essential services. This will facilitate the discovery and mitigation of the sectors' inter-dependencies, and stress-test the coordination and communication capabilities at the national level.

Singapore will:

- **Enhance its national cyber situational awareness by integrating threat discovery, analysis and incident responses.**
- **Conduct regular multi-sector cybersecurity exercises with more complex scenarios and involving more and more sectors. Through these exercises, we aim to identify vulnerabilities due to cross-sector interdependencies and stress-test coordination and communication across sectors.**
- **Build up more National Cyber Incident Response Teams (NCIRT) which can be mobilised to lend support to a sector or CII operator should they face an escalating cyber incident.**
- **Strengthen the Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP) of essential services, especially against a cyber-attack.**

Exercise Cyber Star

Over the past years, the Government has conducted sector level exercises to exercise individual critical sectors in their readiness and incidence response plans against a cyber-attack. This culminated in Exercise Cyber Star, a multi-sector exercise conducted by CSA in March 2016. It brought together industry and Government representatives across the infocomm, Government, energy, and banking and finance sectors to exercise the response to a nationwide attack. The exercise was a milestone in building up cybersecurity readiness and validating the effectiveness of cross-sector cooperation.

Expand the National Cyber Incident Response Team (NCIRT)

National Cyber Incident Response Teams (NCIRT) are currently drawn from the incident response teams from CSA, Government Technology Agency (GovTech), the Ministry of Home Affairs (MHA) and the Ministry of Defence (MINDEF). They are part of the Tier 1 and Tier 2 response under the national cyber response plan.

The Government will further enhance the capability of the NCIRTs to deal with more complex and challenging attack scenarios. It will also build up more NCIRTs by upgrading certain sectoral CIRTs and also consider raising additional NCIRTs from industry and academia. This will increase the national capacity to deal with large scale cyber-attacks.

Recover, Restore, Remediate

Resilience in essential services is especially applicable to CIIs, as a cyber-breach realistically cannot be prevented all the time. A resilient system will need to put in place prevention activities that must be integrated with an expedient incident response plan and a comprehensive recovery strategy to mitigate the effects of cyber incidents. As such, an important aspect following a cyber-attack is to be able to return affected CIIs to normal operations as soon as possible, or to facilitate their continued operations in sub-optimal conditions through a prolonged attack. The Government will work with the sectors to ensure that robust Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP) are built into their CII protection plans.

"We will develop a standalone Cybersecurity Act that provides for stronger and more proactive powers."

Minister-in-charge of Cybersecurity, Dr Yaacob Ibrahim, 2015

STRENGTHEN GOVERNANCE AND LEGISLATIVE FRAMEWORK

The Cybersecurity Act

The Government will introduce a new Cybersecurity Act. This new legislation will equip CSA with the necessary powers to effectively address increasingly sophisticated threats to national cybersecurity.

The new Cybersecurity Act will establish a comprehensive framework for the prevention and management of cyber incidents, and complement the existing Computer Misuse and Cybersecurity Act (CMCA), which will continue to govern the investigation of cybercrime. It will:

- Require CII owners and operators to take responsibility for securing their systems and networks. This includes complying with policies and standards, conducting audits and risk assessments, and reporting cybersecurity incidents. CII owners and operators will also be required to participate in cybersecurity exercises to ensure their readiness in managing cyber incidents; and

- Facilitate the sharing of cybersecurity information with and by CSA. Recognising that cybersecurity breaches will happen despite our best efforts, the Act will empower CSA and sector regulators to work closely with affected parties to expeditiously resolve cybersecurity incidents and recover from disruptions.

CSA has been and will continue to work closely with sector regulators, CII stakeholders and industry players in formulating detailed proposals for the new Act. A key principle is to adopt a risk-based approach to cybersecurity, and to build in sufficient flexibility to take into account the unique circumstances and regulations in each sector.

The need for stronger cybersecurity laws

In 2013, the Government amended the then-Computer Misuse Act to strengthen Singapore's capability in responding to national-level cyber threats. This became the Computer Misuse and Cybersecurity Act (CMCA). When there is an actual or suspected cyber threat, the CMCA empowers the Minister of Home Affairs to direct affected parties to share vital information, and carry out necessary measures to mitigate the impact of the threat. Additionally, some sector regulators have other legislative powers to enforce cybersecurity requirements on their licensees. These powers, however, vary from sector to sector, depending on the operating environment and level of technology adoption in each sector.

Today, cybersecurity threats have become more sophisticated. Essential services around the world, including Singapore's, face a greater risk of being disrupted. In the recent past, cyber perpetrators have demonstrated attacks on a range of essential services, including the power grid and key banking systems. There is a need to implement more robust laws that allow for a more proactive approach to national cybersecurity. Many countries have also strengthened their cybersecurity laws over the past few years, focusing on areas such as standards for essential service providers, information sharing, and cyber crisis management.

SECURE GOVERNMENT NETWORKS

Government systems are among the prime targets for cyber-attackers. Government systems contain sensitive data, including those about their citizens; they may be linked to essential services supplied by CII operators; they are used to support a gamut of public services including the maintenance of national security and sustaining the economy.

Hence, the Government will spare no effort in safeguarding its systems and networks. The Government has undertaken, in this current term, to work towards a goal of setting aside 8 per cent of its ICT expenditure on cybersecurity.

The Government sector is already identified as one of the eleven CII sectors in the national cyber response plan.

The Government's plans as a CII sector lead incorporate many of the elements of the larger national plan. They involve:

- **Reducing the attack surface presented by Government systems and erecting multiple layers of security controls and network segmentation according to vulnerability and need;**
- **Expanding our capacity to detect, correlate and analyse threats, using automation and other technologies; and**
- **Sharpening the skills of our incident responders and stress-testing our systems through more complex and realistic attack scenarios.**

Cybersecurity professionals on duty at Cyber-Watch Centre (CWC)

Reducing Attack Surface

The Government has put in place long-term measures including on-going and proactive reviews of the ICT operating environments, to ensure that security controls are commensurate with rapidly evolving threats. For example, in view of the increased frequency of targeted attacks on Government networks, the Civil Service will separate Internet surfing from the networks that hold classified data according to vulnerability, exposure and need.

At the same time, the Government will continue its approach of adopting new technologies to deliver secure and resilient digital services. It is also looking into risk reduction initiatives to minimise the potential loss of citizens' data or prolonged outages of digital services.

Enhancing Situational Awareness through Technology

The Monitoring and Operations Control Centre (MOCC), Cyber-Watch Centre (CWC), and Threat Analysis Centre (TAC) provide the Government with cyber situational awareness of its networks.

We will continue to invest in technologies such as analytics, automation, artificial intelligence, and other state-of-the-art security technologies. This will maintain the centres' operational excellence, to enable timely detection and response to a cyber incident.

Preparing for Cyber Breaches

The Government has expanded considerable effort in building a team of highly-skilled security incident responders. However, we recognise that no system is 100 per cent fool-proof and breaches may still occur even despite the best of our efforts. We will continue to hold regular cybersecurity exercises to stress test our procedures and capabilities for a realistic evaluation of our proficiency, and conduct red-teaming sessions to validate the security of our systems. The Government will work with the sectors to ensure that CII protection plans are in place for expedient remediation to restore essential services.

Cyber-Watch Centre (CWC)

The Cyber-Watch Centre (CWC) was established by the Info-communications Development Authority of Singapore (IDA) in 2007 to monitor cyber threats to government networks and provide early warning of impending cyber-attacks. To improve the detection of malicious activities which could affect access to online public services, the CWC was upgraded in 2015 with a wider range of detection capabilities and enhanced correlation capabilities.

This is an example of a proactive defence-in-depth security measure to mitigate increasingly sophisticated attacks and enhance infocomm infrastructure security.

CHAPTER 2

A SAFER CYBERSPACE

Digital connectivity has both empowered and endangered businesses and individuals. It opens new social and commercial opportunities, yet also exposes citizens to criminal syndicates across the world. By commandeering computing devices, these malicious actors can steal data, extort money, and attack networks, causing harm to others. Cyberspace needs to be kept safe and trustworthy for businesses and individuals to benefit from it.

Keeping cyberspace safe requires a spectrum of actions from the international to individual levels. Countries have to cooperate to take down criminals operating across borders, while businesses and individuals can take preventive measures to keep their systems and devices safe. Cybersecurity is the collective responsibility of everyone - the Government, businesses, individuals and the community.

The Government will:

Combat cybercrime through the National Cybercrime Action Plan (NCAP). The National Cybercrime Action Plan (NCAP) was launched in July 2016 to establish a coordinated national effort to deal with cybercrime. First, we will **educate and empower** the public to stay safe in cyberspace, as it is more effective to prevent a cybercrime from happening in the first place. Second, we will **enhance the Government's capacity and capability** to combat cybercrime, in view of cybercrime's transnational nature, speed and scale. Next, we will **strengthen legislation and the criminal justice framework**. This will support the investigation of cybercrimes and prosecution of cybercriminals. Finally, we will **step up partnerships and international engagement** to manage the rapidly evolving nature of cybercrime and tackle cross-border issues.

Enhance Singapore's standing as a trusted hub.
We will **build a trusted data ecosystem** by fostering trust between organisations and users for data usage. Next, we will develop Data Protection Officers as a professional career track to support the effective implementation of data protection measures. We will also strengthen Singapore's position as a data hub by facilitating cross-border data flows and introducing Data Protection TrustMarks. Finally, we will work with partners – global institutions, other governments, industry partners and Internet Service Providers – to achieve a cleaner internet by regularly measuring the health of the Internet, identifying cyber threats quickly and **reducing malicious traffic**.

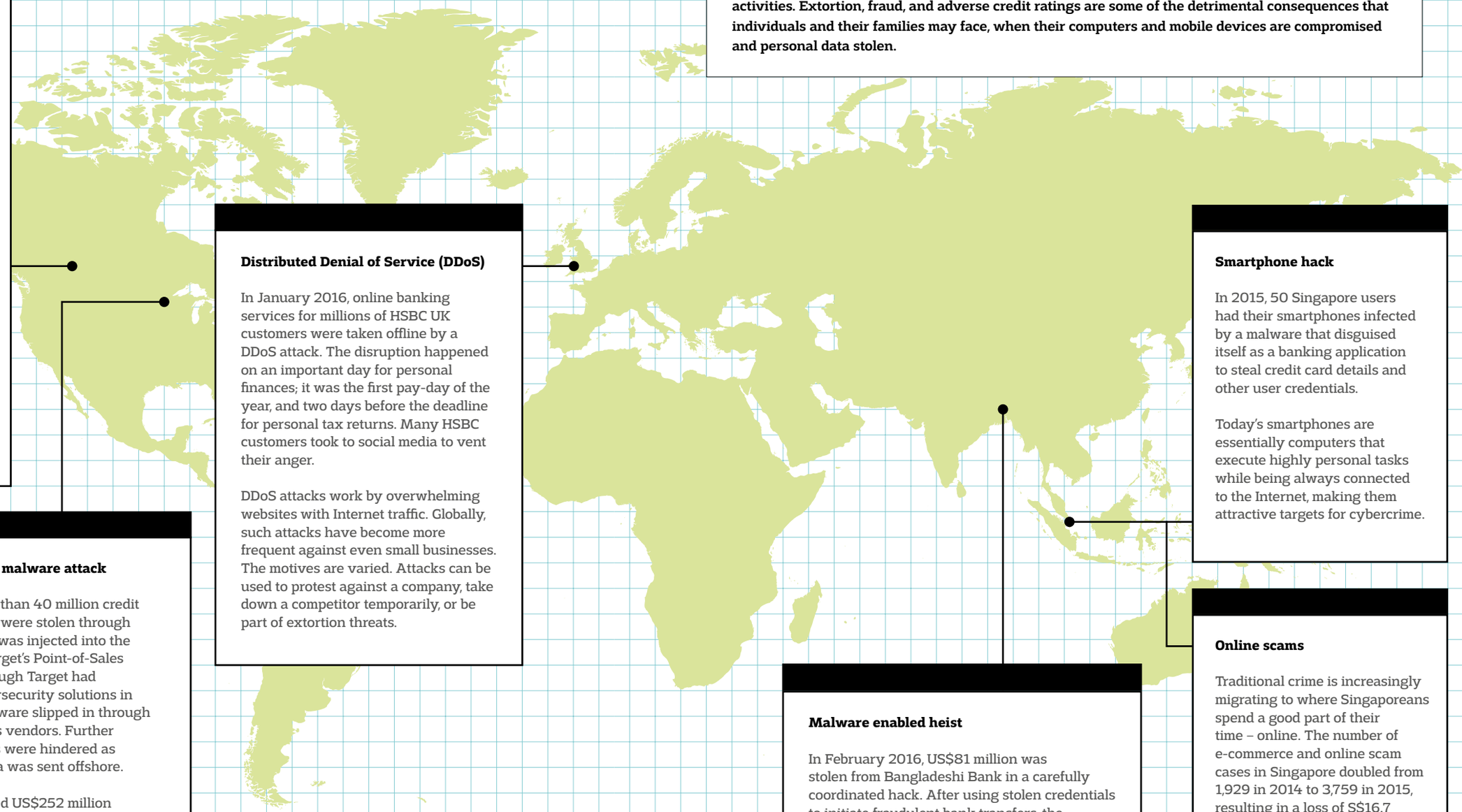
Promote collective responsibility for cybersecurity.
The actions of each business and individual can impact our collective safety in cyberspace. Businesses and individuals need to **stay informed** and take preventive measures to secure their computer systems and digital devices, particularly to prevent malicious actors from hijacking their systems and devices to cause harm to others. Communities and business associations can take the lead to **make cybersecurity a priority**, and **tap on government cybersecurity expertise** to improve their members' understanding of cybersecurity issues and encourage adoption of good practices. With the right knowledge, expertise and attitude, we can all reap the full benefits and possibilities of technology.

CYBERCRIME: THE NEW CRIMINAL FRONTIER

The growth of the Internet has created numerous business and social opportunities. However, where there are opportunities, there are also risks. Locally and internationally, the Internet has been exploited for cybercrimes like scams, hacks and thefts.

For businesses, malicious cyber activities may cause service disruptions and loss of data pertaining to customers, employees, and commercial entities. These can result in substantial revenue losses, erosion of customer goodwill, and loss of reputation. Inextricably, personal lives may also be affected.

For individuals, poor personal cybersecurity habits can open doors to cybercrime and malicious activities. Extortion, fraud, and adverse credit ratings are some of the detrimental consequences that individuals and their families may face, when their computers and mobile devices are compromised and personal data stolen.



Ransomware

In May 2016, ransomware encrypted University of Calgary's computer systems on the eve of a conference. The conference organisers had to re-create processes and conference data by hand for the event to continue. To prevent the malware from spreading to the rest of the systems, the University had to shut down other IT services, causing a week-long, campus-wide disruption that was more far-reaching than the impact of the malware.

The malicious actors behind this incident demanded the equivalent of Canadian $20,000 in Bitcoins to decrypt the data. The University eventually gave in and paid the ransom to retrieve the research data.

Distributed Denial of Service (DDoS)

In January 2016, online banking services for millions of HSBC UK customers were taken offline by a DDoS attack. The disruption happened on an important day for personal finances; it was the first pay-day of the year, and two days before the deadline for personal tax returns. Many HSBC customers took to social media to vent their anger.

DDoS attacks work by overwhelming websites with Internet traffic. Globally, such attacks have become more frequent against even small businesses. The motives are varied. Attacks can be used to protest against a company, take down a competitor temporarily, or be part of extortion threats.

Smartphone hack

In 2015, 50 Singapore users had their smartphones infected by a malware that disguised itself as a banking application to steal credit card details and other user credentials.

Today's smartphones are essentially computers that execute highly personal tasks while being always connected to the Internet, making them attractive targets for cybercrime.

Supply chain malware attack

In 2013, more than 40 million credit card numbers were stolen through malware that was injected into the US retailer Target's Point-of-Sales system. Although Target had multiple cybersecurity solutions in place, the malware slipped in through one of Target's vendors. Further investigations were hindered as the stolen data was sent offshore.

Target incurred US$252 million of breach-related expenses and faced several lawsuits. Target's CEO held himself personally accountable and resigned.

Malware enabled heist

In February 2016, US$81 million was stolen from Bangladeshi Bank in a carefully coordinated hack. After using stolen credentials to initiate fraudulent bank transfers, the hackers used malware to hide the traces of the transactions, hindering remediation actions.

Online scams

Traditional crime is increasingly migrating to where Singaporeans spend a good part of their time – online. The number of e-commerce and online scam cases in Singapore doubled from 1,929 in 2014 to 3,759 in 2015, resulting in a loss of S$16.7 million.

COMBAT CYBERCRIME

National Cybercrime Action Plan (NCAP)

The Internet has afforded criminal elements the opportunity to commit cybercrimes quickly, easily and on a large scale. Criminals have also exploited the anonymity provided by the Internet and the transnational nature of cybercrime to escape detection and prosecution. These characteristics of cybercrime pose significant challenges for law enforcement agencies around the world.

As the use of the Internet becomes more prevalent in Singapore, the number of cybercrime cases has risen sharply. Recognising the need for a concerted and coordinated national effort to effectively deal with the cybercrime, the Ministry of Home Affairs (MHA) launched the National Cybercrime Action Plan (NCAP) in July 2016.

The NCAP sets out the Government's key principles and priorities in combating cybercrime. The Plan also details the Government's ongoing efforts and future plans to tackle cybercrime. The vision of the NCAP is to ensure a safe and secure online environment for Singapore.

The NCAP has four priority areas:

A Educating and empowering the public to stay safe in cyberspace

Prevention is the best way to combat cybercrime; the majority of cybercrimes can be prevented if businesses and individuals are educated on the risks of cybercrime and adopt simple cybercrime prevention measures to protect themselves online.

(i) Conducting outreach to the general public

In order to educate and empower the public to stay safe in cyberspace, the Singapore Police Force (SPF) regularly shares cybercrime prevention messages with the public via various media platforms, such as television, newspapers, social media, text messages and posters at public transport nodes and lifts in public housing blocks. At the local community level, SPF's Neighbourhood Police Centres frequently engage the residents through Community Safety & Security Programmes and roadshows. Through its Public Cyber-Outreach & Resilience Programme (PCORP), SPF uses behavioural insights to nudge the general public to adopt good cyber hygiene practices.

(ii) Engagement of vulnerable groups in society

SPF has also tailored its cybercrime prevention outreach programmes to match the profile of different vulnerable groups in society, thereby ensuring that the message of cybercrime prevention is effectively communicated to all segments of society. Through its Collaborative Social Programme (CoSP), SPF will work with schools and Non-Governmental Organisations (NGOs) to raise cybercrime prevention awareness among vulnerable groups.

(iii) Providing a one-stop self-help portal against scams

SPF has worked with the National Crime Prevention Council (NCPC) to transform the Scam Alert website (www.scamalert.sg) into a one-stop self-help portal against scams. The portal will provide information to the public on the different types of scams, and empower the public to take steps to guard against them.

B Enhancing the Government's capacity and capability to combat cybercrime

The transnational nature of cybercrimes, coupled with the speed and scale at which such crimes are perpetrated, presents formidable challenges for traditional law enforcement approaches. In order to effectively combat cybercrime, the Government will (i) establish the SPF Cybercrime Command, (ii) boost cybercrime investigation capabilities, (iii) equip public officers with the relevant skills to combat cybercrime, and (iv) enhance coordination between SPF and government agencies.

(i) Establishing the SPF Cybercrime Command

The SPF Cybercrime Command was established in December 2015 to increase the agility and effectiveness of the SPF to respond to cybercrimes by integrating SPF's cyber-related investigation, forensics, intelligence and crime prevention capabilities within a single command.

(ii) Boosting cybercrime investigation capabilities

SPF has also embarked on several technology initiatives to improve its cybercrime investigation capabilities. These efforts will enable SPF to effectively investigate the rising number of cybercrime cases and quickly process large volumes of digital information in order to sieve out necessary evidence for a successful prosecution.

One such initiative is the DIGital Evidence Search Tool (DIGEST) that will automate the forensic processing of voluminous data. This will in turn lighten the workload of investigation officers and allow them to focus their efforts on more specialised investigation functions. The tool will also reduce the processing time for digital evidence, ensuring that investigation officers can follow up on leads expeditiously and solve cases in a shorter time.

(iii) Equipping public officers handling sensitive data with the relevant skills to combat cybercrime

In recognition of growing cybersecurity and cybercrime threats, the Centre for Cyber Security Studies (CCSS) was established in 2014 within the Home Team Academy (HTA). The CCSS facilitates the capability and capacity development of Home Team Departments and key stakeholders responsible for the protection and operations of infocomm systems across the public sector. One of CCSS' core functions is to equip Home Team officers with the necessary skills to deal with cybercrime. To achieve this, a Cyber Security Lab (CSL) has been set up in the CCSS as a modern hands-on facility for familiarising trainees on approaches to mitigate cyber threats and investigate cyber incidents. CCSS will expand its curriculum to offer a variety of skills-based courses, ranging from cybersecurity fundamentals and cyber defence, to incident response, digital forensics and malware analysis. These courses are tailored to the needs of officers, depending on their professional roles and competency requirements.

(iv) Strengthening coordination between SPF and government agencies

SPF also works closely with its partner agencies to ensure a coordinated response to cybercrimes. In recent years, AGC and SPF have worked closely together on sensitive and high-profile cybercrime cases, coming together right from the start of the investigations. AGC's expertise has helped SPF to ensure that crucial evidence is secured at an early stage and that police investigations are watertight.

Given the closely-related nature of cybersecurity and cybercrime, SPF and CSA will work together to ensure an effective response to cyber-related incidents and conduct exercises to stress-test existing workflows, coordination arrangements and procedures.

C Strengthening legislation and the criminal justice framework

The investigation of cybercrimes and prosecution of cybercriminals must be supported by a robust criminal justice framework. Laws need to be updated to deal with new cyber-offences and traditional crimes committed online. Regulatory frameworks have to be constantly strengthened to prevent criminals from taking advantage of loopholes.

(i) Amending the Computer Misuse and Cybersecurity Act

MHA intends to amend the Computer Misuse and Cybersecurity Act (CMCA), to ensure that the Act continues to be effective in dealing with the transnational nature of cybercrimes, as well as the evolving tactics of cybercriminals.

(ii) Reviewing other laws

In addition to amending the CMCA, MHA will review other related laws such as the Criminal Procedure Code to ensure that these laws remain relevant in dealing with traditional crimes that are committed in cyberspace.

(iii) Strengthening regulatory frameworks

Aside from public education and outreach, a key method of cybercrime prevention is to increase the difficulty of committing such offences by plugging potential loopholes in digital platforms and processes. MHA will regularly review regulatory frameworks, to ensure that cybercriminals are not able to exploit vulnerabilities in technology.

Prevention is key in countering the threat of cybercrime

The scale and complexity of cybercrime will continue to grow, with its transnational nature posing legal and operational difficulties for law enforcement agencies. Prevention is therefore still the key strategy to counter the threat of cybercrime. The NCAP will prioritise educating and empowering the public to be safe in cyberspace. Through the various initiatives in the NCAP, the Government will build strong partnerships with industry, IHLs and the public, and forge a sense of shared responsibility in the fight against cybercrime.

D Stepping up partnerships and international engagement

Industry and Academic Partnerships

Deep expertise to deal with cybercrimes need not just reside with the Government and can be found within the private sector and academia. Given the rapidly evolving nature of cybercrime, the Government will work closely with industry players and Institute of Higher Learning (IHLs) so that the necessary information and expertise to deal with the latest threat posed by cybercrime can be shared seamlessly.

(i) Increasing cybercrime awareness in the private sector

MHA has partnered industry and IHLs to increase awareness of cybercrimes in the private sector. SPF regularly engages key private sector stakeholders, such as those from the Infocomm Technology and banking industries to enhance cybercrime prevention efforts, raise awareness of cybercrimes and encourage the adoption of good cyber hygiene practices.

(ii) Developing capabilities to combat cybercrime

The Government has also collaborated with the private sector to jointly develop capabilities to respond to the latest cyber threats. For instance, SPF has partnered local research institutes to develop new cybercrime investigations and forensics capabilities. MHA has also worked with IHLs to create conducive environments for the development of cyber-related innovations. One example is MHA and Temasek Polytechnic's joint establishment of the Temasek Advanced LEarning, Nurturing and Testing (TALENT) Lab, which serves as a platform for IHL students to design and validate innovations, to see if they are effective in dealing with cyber-threats.

International engagement

Strong international partnerships enable countries to deal with cybercrime more effectively. Singapore will actively foster regional and global cooperation, partner INTERPOL and other countries in capacity building initiatives, and bring global experts and thought leaders together to discuss the latest threats, trends and solutions in the cyber domain, and share best practices and solutions.

(i) Fostering regional and global cooperation

Singapore is at the forefront of working with foreign countries to enhance our operational cooperation against cybercrime. At the regional level, Singapore is the Association of Southeast Asian Nations (ASEAN) Voluntary Lead Shepherd on Cybercrime. This provides a platform for the ASEAN Member States (AMS) to coordinate the regional approach to cybercrime, and work together on capacity building, training and the sharing of information. At the international level, Singapore hosts the INTERPOL Global Complex for Innovation (IGCI), INTERPOL's global hub on cybercrime. Singapore has led the IGCI Working Group and INTERPOL Operational Expert Group on Cybercrime, working with other INTERPOL member countries to define INTERPOL's cybercrime programme. Singapore will leverage INTERPOL's resources to strengthen our global operational networks and build new capabilities to tackle cybercrime.

(ii) Building capacities and capabilities through collaboration at the regional and global levels

Singapore has rolled out several programmes with partner countries and INTERPOL. This includes the two-year (2016 – 2018) ASEAN Cyber Capacity Development Project funded by Japan and implemented by INTERPOL, the Singapore-United States Third Country Training Programme, and the ASEAN Plus Three Cybercrime Workshop, involving the People's Republic of China, Japan and the Republic of Korea. The involvement of key Asian partners, AMS and INTERPOL facilitates a conducive environment for collaboration on cybercrime issues and sharing of best practices, and forging of effective operational links between countries and across the regions.

(iii) Bringing global experts and thought leaders together

Since 2013, Singapore has been supporting thought leadership platforms that bring together public sector and industry partners on cybercrime. One such example is the RSA Conference Asia Pacific and Japan (RSAC APJ). Held annually in Singapore, the RSAC APJ is Asia Pacific's leading conference on information security.

ENHANCE SINGAPORE'S STANDING AS A TRUSTED HUB

Build a trustworthy data ecosystem

The compromise of personal data can cause adverse disruptions to the affected individuals and businesses. With increasing amounts of data migrating to computer systems and electronic devices, there is a need to secure these systems and safeguard individuals' data against theft and misuse. At the same time, organisations can leverage good personal data management to gain a better understanding of their customers, increase business efficiency and effectiveness, and boost customer confidence.

Trust is essential for a data-enabled economy and society. To build a trusted data ecosystem, our organisations have to shift from compliance to accountability.

Singapore will:

- Work with organisations to embrace data protection as part of their corporate culture;
- Professionalise Data Protection Officers to support the effective implementation of data protection measures; and
- Enhance Singapore's standing as a trusted data hub by introducing Data Protection Trustmarks and working with foreign Data Protection Authorities to facilitate cross-border data flows.

Build a relationship of trust

A reliable and robust data ecosystem promotes trust and innovation. To help organisations take ownership in promoting trust and adopting a mindset of accountability, the Personal Data Protection Commission (PDPC) will develop a Data Protection Management Programme to help organisations embrace data protection as part of their corporate culture. Robust data protection processes are needed to enable organisations to better use data. To do so, organisations should adopt a Data-Protection–by-Design approach, which factors data protection as a key consideration in the early stages of any product or service development. The rigour of this framework will also require that businesses conduct Data Protection Impact Assessment as part of the design, rollout and review of systems, applications and business processes. Given that data breaches can and will still happen despite organisations' best efforts at securing personal data, PDPC is studying a mandatory breach notification for serious data breaches.

Personal Data Protection Seminar 2016

Professionalise Data Protection Officers

Today, Data Protection Officers (DPOs) hail from a range of occupations. PDPC will develop a Data Protection Competency Framework (DPCF) to grow DPOs as a professional career dedicated to overseeing data protection requirements of organisations. This will ensure that DPOs are equipped with the relevant skills, competencies, and certifications needed to do their jobs.

Enhance Singapore's standing as a trusted data hub

PDPC is currently developing a system of Data Protection Trustmarks to certify organisations' data protection processes. By helping organisations gain mutual confidence in each other's transactions involving personal information, the Trustmarks will increase compliance and reinforce Singapore's standing as a trusted data hub.

Another focus area is the facilitation of cross-border data flows. PDPC will identify areas of collaborations and cooperation with well-established foreign Data Protection Authorities. It will participate in global multilateral networks to mutually recognise the adequacy of each economy's data protection laws, thus enabling transfers of data across jurisdictions.

Ongoing efforts for personal data protection

Under the Personal Data Protection Act (PDPA), organisations are to take reasonable steps to manage and secure personal information that they hold. Today, the PDPC adopts a multi-pronged approach in supporting organisations, particularly the Small and Medium-sized Enterprises (SMEs). Through industry briefings, online training resources, and advisory guidelines, SMEs are equipped with information on the requirements of the PDPA and good data management practices to adopt.

Cleaner Internet

The Internet's ability in allowing anyone to send large volumes of any form of information – data, voice, video - to another user has propelled it to be the world's dominant communication platform. However, this design exposes end-users' machines to malicious software that can hijack these devices to blast phishing emails and even launch cyber-attacks.

The increasing number of infected machines spewing malicious traffic into the Internet has made cyberspace less safe for everyone. Just as we would stop people who eject sewage into clean water pipes, we will also have to block users who may be unwittingly polluting the Internet pipeline and alert them on measures for cleaning up their machines.

As "gatekeepers" managing the Internet gateways and enabling information flows across the Internet, local Internet Service Providers (ISPs) play an essential role to achieve a safer Internet space. In 2011, the Government issued the first Secure and Resilient Internet Infrastructure Code of Practice to designated ISPs to ensure that sound security is in place to deal with current and emerging cyber threats. The Info-communications Media Development Authority (IMDA) will continue working with the ISPs to secure Internet infrastructure for businesses and individuals.

Singapore will join the global community to measure and improve the health state of cyberspace, and CSA will collaborate with international organisations on this front. To complement these efforts, the Singapore Computer Emergency Response Team (SingCERT) will continue to obtain early warning of cyber threats and alert users on the preventive measures they can adopt.

PROMOTE COLLECTIVE RESPONSIBILITY

The prevalence of ICT and the Internet has transformed the way we work, play, live, learn and connect with one another. Just as we lock our doors and keep our keys safe in the physical world, we have a similar responsibility to stay safe in the cyber world. Individuals now keep more of their friends' and families' personal data than ever before on personal devices. The stakes are higher for businesses as they are custodians of computerised data that are vital to operations and impact customers' lives. Cybersecurity is a collective responsibility and a way of putting Total Defence into action to keep Singapore safe. Everyone, whether individuals or businesses, has a role in creating a safer cyberspace.

"Having strong security technology is not enough [...] training employees in cybersecurity is critical. "

Mr Teo Siong Seng,
Singapore Business Federation
Chairman, 2015

National Security Conference 2015, In Conversation - How ready are Singapore Companies?

Stay informed

Recognising that businesses and individuals can reduce cyber incidents by taking basic measures, the Government has taken steps to educate the public on cybersecurity since the first Infocomm Security Masterplan was launched in 2005. This needs to be a continuous effort as "old" technology gets upgraded with smart features. Today, 8 in 10 Singapore residents install anti-virus software on their computers but only 3 in 10 do so on their smartphones[2].

CSA will keep the public updated on new cybersecurity measures to keep pace with technological changes. We will continue existing outreach programmes such as the Cybersecurity Awareness Campaign which started since 2011. We will also broaden their reach across age groups, and to include both individuals and businesses. We will leverage national security awareness building platforms such as the Total Defence and Let's Stand Together campaigns to raise appreciation of the role of cybersecurity for a strong and prepared nation. We will expand the range of resources on the GoSafeOnline web portal and other critical social media platforms.

Public education can be more effective through collaborative projects across the government, industry and community. The Inter-Ministry Cyber Wellness Steering Committee brings cyber-wellness messages to youths and has reached more than 245,000 participants through 25 supported projects since 2009. Another example is the Cyber Security Awareness Alliance, which brought together government agencies, private enterprises, and professional associations to promote the adoption of essential cybersecurity practices. Since its formation in 2008, the Alliance has reached out to various audiences through exhibitions, clinics and talks.

Make cybersecurity a business priority

For sustained and sustainable cybersecurity adoption, cyber risks should be recognised and treated as important business risks. Trade Associations and Chambers (TACs) play an important role in reaching out to businesses.

Trade Associations and Chambers (TACs) play an important role in improving the cybersecurity of their members' business operations. The Government will continue engaging TACs to help their members tap on grants and resources to adopt cybersecurity measures and develop cybersecurity capabilities. We will also work with TACs to advocate the Security-by-Design approach and incorporate cybersecurity holistically into business risk management.

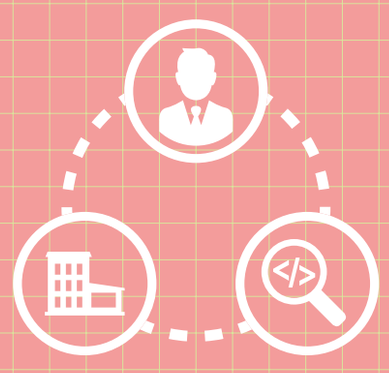
Tap on government cybersecurity expertise

Businesses may find it challenging to keep pace with new cyber threats. SingCERT, which was set up in 1997 to facilitate the detection, resolution and prevention of cybersecurity related incidents, will deepen its threat discovery and analysis capabilities to deal with the evolving local cyber threat environment. SingCERT will expand its capacity to facilitate the sharing of cybersecurity information with the business community, while ensuring that sensitive corporate and personal data are protected. It will also partner the industry and Institutes of Higher Learning (IHLs) to support cybersecurity resource centres for businesses and individuals.

[1] The Singapore Government introduced Total Defence in 1984 as a concept to involve every Singaporean in playing a part, individually and collectively, to build a strong, secure and cohesive nation. It involves all Singaporeans in the following five aspects: military defence, civil defence, economic defence, psychological defence and social defence.
[2] Infocomm Development Authority (IDA) Infocomm Usage by Households and Individuals Survey 2014
[3] Ministry of Education (MOE) Press Release on 7th Call for Proposals on Cyber Wellness Projects

CHAPTER 3

A VIBRANT CYBERSECURITY ECOSYSTEM



With its advanced infrastructure and tech-savvy workforce, Singapore is well-positioned to develop a vibrant cybersecurity ecosystem comprising highly skilled professionals, companies with deep cybersecurity capabilities and strong translational research and development (R&D).

The ecosystem will ensure a sustainable source of expertise and solutions to support our plans for a resilient national infrastructure and a safer cyberspace. It will also bring economic opportunities to Singaporeans and Singapore-based companies. Singapore's cybersecurity industry is dynamic and fast-growing, and has the potential to double in value by 2020. Furthermore, integrating cybersecurity service offerings with industry sectors that Singapore is traditionally strong in will enhance our competitive advantages in these areas.

The Government will work with industry partners, professional associations, IHLs and research institutes in three main areas.

We will:

Establish a professional workforce. We will encourage existing cybersecurity professionals to develop their careers in the industry by defining **clearer career pathways**, promoting **internationally-recognised certifications**, and building **strong communities of practice**. To grow the workforce, we will attract promising students through **scholarship and sponsorship programmes**. We will also support new entrants to the profession **through industry-oriented curriculum** for students as well as **up-skilling and re-skilling opportunities** for mid-career professionals.

Extend Singapore's cybersecurity advantage through strong local companies. We will build up the industry by **attracting and anchoring companies** with advanced capabilities. We will also **nurture start-ups** to boost the development of niche and advanced solutions and **grow local champions** to sustain strategic areas of interest. We will also **develop market opportunities** to bring made-in-Singapore solutions into the global market.

Innovate to accelerate the industry's growth. The **National Cybersecurity R&D Programme** has set aside S$190 million from 2013 to 2020 to support research into both technological and human-science aspects of cybersecurity. We will sustain this effort with **world-class R&D facilities and focused talent development programmes**. We will promote **R&D collaborations between the Government, academia and industry** to engender faster and more market-relevant R&D outcomes.

ESTABLISH A PROFESSIONAL CYBERSECURITY WORKFORCE

Good security requires highly-skilled practitioners with deep expertise. Today, there is a shortage of cybersecurity manpower around the world. Qualified professionals are in great demand as businesses pay more attention to cyber risks. This demand will only increase as the frequency and consequences of cyber threats continue to grow. To ensure that Singapore has an adequate and well-trained cybersecurity workforce, Singapore will:

- **Encourage existing professionals to remain and further their development in the industry. We will institute clear career pathways, promote certification, and foster strong communities of practice; and**
- **Work with industry and IHLs to attract new graduates and convert existing professionals from related fields. IHLs will update their curriculum to be relevant to industry needs so as to facilitate the transition of new entrants to the workforce. We will offer cybersecurity scholarships and sponsorships to attract promising students. We will also offer up-skilling and re-skilling opportunities to cross-train mid-career professionals in cybersecurity for better job prospects.**

The cybersecurity profession is fast-paced and varied. There are opportunities to specialise in different areas. These include incident response, digital forensics and penetration testing for the technically inclined; threat and intelligence analysis for the analyst-at-heart; and risk management and governance for the methodical change drivers. Regardless of specialisation, cybersecurity professionals from entry-level to C-suite positions are highly sought after as companies across many industries seek to secure their systems and data. The Government is committed to developing the cybersecurity industry as a source of good jobs for Singaporeans.

New entrants to the cybersecurity workforce will be supported by:

Industry-oriented Curriculum

Our universities and polytechnics already offer cybersecurity programmes for those keen to pursue a cybersecurity education. For example, the Singapore Institute of Technology (SIT) offers a Bachelor of Engineering with Honours in Information and Communications Technology (Information Security), and Singapore University of Technology and Design (SUTD) offers a Masters in Cybersecurity. The Government will work with Institutes of Higher Learning (IHLs) and industry partners to ensure that these programmes and curriculums continue to be relevant to the industry, with students learning and acquiring practical skills.

In particular, the Ministry of Education (MOE) is launching a co-operative degree programme where students alternate between campus and company on a semester basis. The programme enables students to develop a deeper and practical understanding of their field of study by integrating work and study. Students may even be hired by the company from the outset. CSA will be one of the participating agencies in this programme and will be working with the partner universities to develop the cybersecurity degree curriculum and provide on-the-job training to successful applicants.

6th Singapore Cyber Conquest, Winner

Scholarship and Sponsorship Programmes

To strengthen the branding of cybersecurity, the Government will build on existing scholarship and sponsorship programmes. Overseas cybersecurity scholarships will be offered to promising students, and students with outstanding performance in IHLs will be given opportunities to further their education.

Up-skill and Re-skill Opportunities

We will facilitate the conversion of professionals in related fields to cybersecurity by building on the existing Cyber Security Associates and Technologies (CSAT) programme. In line with SkillsFuture, these professionals will be able to up-skill and re-skill themselves and be cross-trained in cybersecurity for better job prospects.

Current professionals can look forward to:

Defined Career Trajectory

The growth of a capable, adept and competent workforce is sustained by attractive career prospects and a respected professional status. The Government will work with the industry to define a competency framework for cybersecurity professionals and it will be incorporated into the upcoming SkillsFuture Framework[4] to be launched in 2017. This will allow professionals and employers to determine the types of skills and competencies required for different cybersecurity jobs, and to establish relevant training programmes and clearer career pathways accordingly.

Companies are also encouraged to work with the Government to help cybersecurity professionals develop complementary skills such as risk management and communication. These will facilitate professionals in translating cybersecurity issues into enterprise risk considerations, and bring cybersecurity discussions into the boardroom. Larger companies could also define apex cybersecurity positions at the C-suite level.

To further improve the standing of cybersecurity professionals, the Cyber Security Agency of Singapore (CSA) will work with industry partners to reach out to more companies, especially Small and Medium-sized Enterprises (SMEs), to increase their awareness of what cybersecurity professionals do, and how they can contribute.

The Government will take the lead in introducing a cybersecurity scheme of service for the public sector, with competitive remuneration and progression prospects. It will also train and develop cybersecurity specialists across the public sector.

Internationally-recognised Certifications

Cybersecurity professionals should deepen their skills and keep abreast of evolving technologies and best practices. One way to do so is to adopt internationally-recognised certifications in areas such as digital forensics, malware analysis and incident response. CREST Singapore (Council of Registered Ethical Security Testers), for example, offers certification for practising penetration testers in Singapore.

Strong Communities of Practice

To build a common identity and foster trust within the profession, the Government will work with industry associations such as the Association of Information Security Professionals (AISP) to introduce and build strong Communities of Practice for cybersecurity professionals in Singapore.

[4] The Skills Framework is part of SkillsFuture, a national movement initiated by the Singapore Government in 2015 to help Singaporeans in skills development and skills mastery for the future.

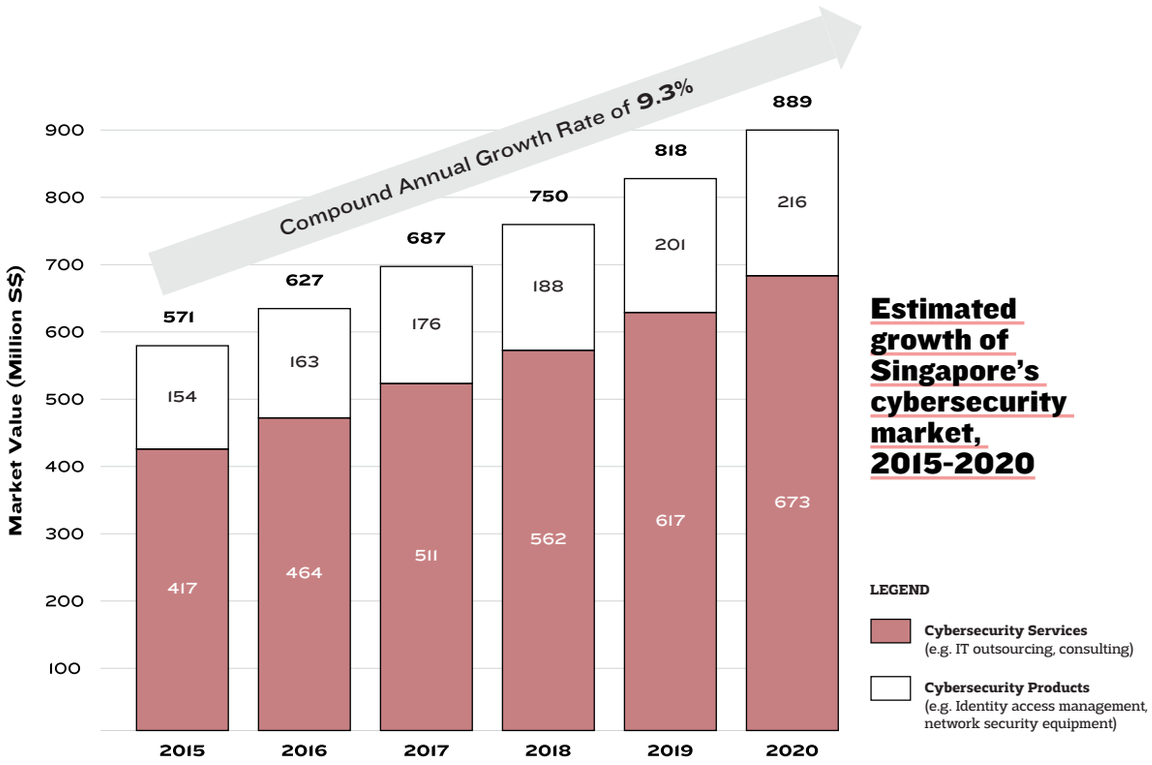
EXTEND SINGAPORE'S CYBERSECURITY ADVANTAGE

Singapore is home to many leading global cybersecurity companies and an emerging cluster of local start-ups. The cybersecurity market in Singapore is worth about S$570 million today, based on estimates by PwC. It has the potential to double in value by 2020, with growth in segments such as identity access management, infrastructure protection and services. Singapore is well positioned within ASEAN and its population of 625 million to support the growing demand for cybersecurity products and services.

The Government is committed to building up Singapore's cybersecurity industry. Besides ensuring that best-in-class cybersecurity solutions are available to the Government and companies in Singapore, a vibrant cybersecurity industry will enhance Singapore's traditional strengths in areas such as financial and infocomm services. These developments will translate to better job opportunities for cybersecurity professionals in Singapore.

To build a vibrant cybersecurity industry, Singapore will:

- **Attract and anchor companies with advanced capabilities in Singapore to inject know-how and dynamism into the local cybersecurity community;**
- **Support start-ups to boost the development of niche and advanced solutions;**
- **Partner with local companies that possess strategic cybersecurity capabilities to develop advanced solutions for Singapore; and**
- **Develop opportunities for made-in-Singapore solutions in the global market and facilitate access to new market segments.**



Estimated growth of Singapore's cybersecurity market, 2015-2020

Source: PwC analysis, Gartner, PwC interviews, desk research.

Attract and Anchor Advanced Capabilities

The Government will leverage Singapore's economic hub status and attract world class cybersecurity companies to base advanced operations, engineering and R&D activities in Singapore. This will increase our access to cutting-edge cybersecurity capabilities and create good jobs for Singaporeans. The Government will also work with these top companies and local champions to strengthen the cybersecurity of our critical sectors and facilitate knowledge exchange to build up local expertise.

Support Start-ups

Singapore's cybersecurity ecosystem will benefit from more start-ups that diversify the industry and boost the development of niche and advanced solutions. The Government and industry will work together to support a strong network of venture capitalists, accelerators and entrepreneurs to help Singapore-based cybersecurity start-ups to grow and scale. This will assist in bringing ideas to the market easily and quickly.

Grow Local Cybersecurity Champions

The Government will grow local cybersecurity champions who can develop globally competitive capabilities in strategic areas of interest and sustain the long-term growth of a competent, professional workforce. The "Partnership for the Advancement of the Cybersecurity Ecosystem" (PACE) programme, initiated by CSA in 2016, is an example of a meaningful public-private partnership that co-develops customised solutions with industry partners for raising our cybersecurity posture while supporting workforce skills development.

Develop Market Opportunities

We will facilitate access to new market segments for our cybersecurity companies and promote Made-In-Singapore solutions. Government and industry will collaborate to set up a cybersecurity resource centre for users to explore and adopt innovative solutions. Together, we aim to bring Singapore's cybersecurity capabilities to the global market.

INNOVATE TO ACCELERATE

For Singapore to be at the cutting-edge of cybersecurity, strong R&D capabilities, institutions and partnerships are necessary. These contribute to the building of resilient infrastructure and the generating of new economic activities.

New cybersecurity solutions must be tested in the real world as part of their development process. Singapore is an ideal test-bed, as a small and agile city state with strong rule of law. Pilot solutions can be quickly implemented and scaled in Singapore. Companies and research labs can leverage Singapore's global position in sectors such as finance and logistics to develop solutions with international significance. As these developed sectors will seek to innovate, they could also serve as ready markets to test new cybersecurity products and solutions.

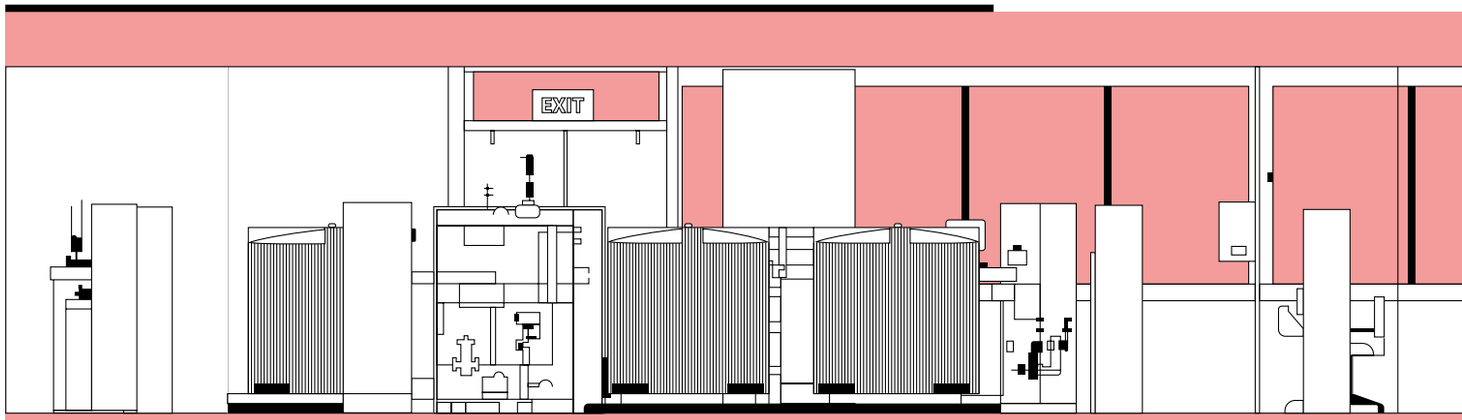
Singapore will:

- **Support research into both technological and human-science aspects of cybersecurity through the S$190 million National Cybersecurity R&D (NCR) Programme;**
- **Establish world-class facilities in specialised research areas and develop local talent to sustain the community; and**
- **Collaborate more closely with academia and industry under the NCR Programme to develop innovative ideas and enhance translational capabilities. A stronger public-private partnership will ensure that R&D can address real-world problems in a more targeted manner, and move research products more quickly from the lab to the market.**

New R&D Facilities

Our universities play a central role in R&D. Each university will become a cybersecurity centre of excellence, and we see each already developing its own area of specialisation. For example, the Singapore University of Technology and Design (SUTD) has a strong focus on cyber-physical systems, and the Singapore Management University (SMU) specialises in mobile security.

In 2016, we also saw the launch of several public-private initiatives, such as the ST Electronics-SUTD Cyber Security Laboratory developed under the Corporate Laboratory @ University scheme administered by the National Research Foundation (NRF). This laboratory brings together industry and academia under one roof to perform cutting-edge cybersecurity research.



The Secure Water Treatment (SWaT) at SUTD is funded by the Ministry of Defence and NRF. It will serve as a key asset for researchers in Singapore and abroad who are studying the design of secure cyber-physical systems.

National Cybersecurity R&D Programme

Singapore's cybersecurity R&D journey has already started, with the aim of translating R&D capability in Singapore into operational strengths. The S$130 million NCR was launched in 2013 by the National Research Foundation (NRF). This was further topped up in 2016 by an additional S$60 million as part of the Research, Innovation and Enterprise 2020 Plan (RIE 2020). The NCR Programme has already awarded 13 projects covering research areas such as cyber-physical systems security and forensics.

World-Class R&D Facilities and Focused Talent Development

Singapore will continue to establish world-class R&D facilities in specialised research areas to attract top researchers and international collaborators, and will promote the shared use of such facilities. The Government is funding S$8 million towards the National Cybersecurity R&D Laboratory at the National University of Singapore (NUS) that will be a shared resource for cybersecurity researchers from academia, industry and the Government. We will also set up programmes to groom local talent for a sustainable and vibrant R&D community.

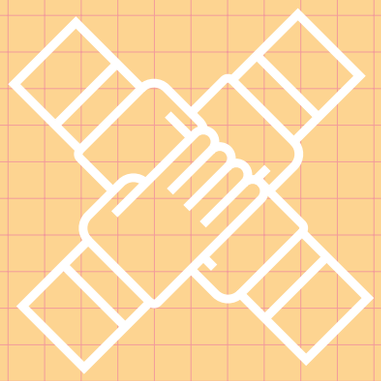
R&D Collaborations between Government, Academia and Industry

Public and private sector agencies can embark on new R&D projects to examine and address complex problems impeding the cybersecurity industry's growth. One example is the Cyber Risk Management (CyRiM) project on cyber risk insurance, which was launched in 2016 by the Nanyang Technological University (NTU) with sponsorship support from the Monetary Authority of Singapore (MAS) and a consortium of insurance industry players. The project brings together academic expertise, industry knowledge, and policy know-how to address the data and standards gaps required for an efficient cyber risk insurance market place.

The Government will initiate a Cybersecurity Consortium, with S$1.5 million in funding over three years from 2016. This Consortium will bring together Government, industry and academia to collaborate on research and seek out viable and practical solutions with commercialisation potential.

CHAPTER 4

STRONG INTERNATIONAL PARTNERSHIPS



Cyber threats do not respect sovereign boundaries and cyber-attacks can emanate from almost anywhere in the world.

Malicious actors have deliberately exploited jurisdictional gaps between countries to their advantage.

Moreover, with countries increasingly connected to one other through trade, global logistics and financial markets, cyber-attacks disrupting one country can and do have serious spill-over effects on other countries. International collaboration in cybersecurity is thus pivotal to our collective security.

Singapore has been an active participant at international platforms on cybersecurity. As an ASEAN member, we have supported and contributed to regional efforts to build cybersecurity capabilities.

Through consensus, agreement, and cooperation, cyberspace can be a safer and more secure place for all.

To achieve this, Singapore will:

Forge international and ASEAN cooperation to counter cyber threats and cybercrime. We will continue working closely with the international community and ASEAN partners to strengthen platforms and procedures for cyber incident reporting and response. We will work with ASEAN Member States to coordinate the regional approach to cybercrime. We will also leverage INTERPOL's resources to tap the global operational networks and capabilities to tackle cybercrime.

Champion international and ASEAN cyber capacity building initiatives in operational, technical, legislative, cyber policy and diplomatic areas. We will partner the international community, Dialogue Partners and ASEAN Member States to organise workshops, seminars and conference that seek to advance cooperation and build capabilities in these aspects .

Facilitate exchanges on cyber norms and legislation.
We will continue to participate in global and regional discussions on cyber norms, cyber policy and legislation, cyber deterrence, and cybercrime cooperation. We will host an annual Singapore International Cyber Week (SICW) – with the inaugural session in October 2016 – to catalyse, stimulate and promote exchanges on cybersecurity and cybercrime issues.

FORGE INTERNATIONAL AND ASEAN COOPERATION TO COUNTER CYBER THREATS AND CYBERCRIME

ASEAN Regional Forum Seminar, 2015: "Operationalising Cyber Confidence Building Measures"

The lightning-fast speed of cyber-attacks requires quick and coordinated actions both at national and international levels. Singapore will work closely with the international community and ASEAN partners to strengthen the platforms and procedures for reporting cyber incidents, sharing information and responding to possible breaches.

Singapore will also partner international organisations like INTERPOL to tackle cybercrime and the Asia Pacific Computer Emergency Response Team (APCERT) to enhance cyber incident reporting and response linkages.

For example, the INTERPOL Global Complex for Innovation (IGCI), which is based in Singapore, provides global training and coordinates international operations on cybercrime for all INTERPOL member countries. Singapore is well-positioned and committed to cooperating with the IGCI and other countries through INTERPOL to conduct cross-border joint operations against cyber criminals[5].

Singapore will continue to contribute at existing ASEAN channels for cooperation such as the annual ASEAN CERT Incident Drill (ACID), ASEAN Network Security Action Council (ANSAC), ASEAN Regional Forum (ARF) Mechanisms as well as ASEAN cybersecurity and cybercrime workshops.

Channels for cooperation

The **ASEAN Regional Forum (ARF)** was established in 1994 to foster constructive dialogue and consultation on political and security issues of common interest and concern, and to make significant contributions towards confidence building and preventive diplomacy in the Asia-Pacific region.

The multi-stakeholder **ASEAN Network Security Action Council (ANSAC)** was set up in 2012 to promote CERT cooperation and sharing of expertise.

The **ASEAN CERT Incident Drill (ACID)** is an annual exercise aimed at strengthening cooperation among CERTs in ASEAN and its Dialogue Partners. The exercise tests the coordination amongst the incident response teams and their incident handling procedures. Singapore has convened ACID since 2006.

[5] Further details on Singapore's international engagement efforts in dealing with cybercrime are found in the National Cybercrime Action Plan (NCAP), launched by the Ministry of Home Affairs in July 2016. The NCAP is available at www.mha.gov.sg.

CHAMPION INTERNATIONAL AND ASEAN CYBER CAPACITY BUILDING INITIATIVES

Cyber threats are borderless and no country can deal with the rapidly evolving threat landscape alone. Singapore stays committed to build cybersecurity capacity within ASEAN in operational, technical, legislative, cyber policy and diplomatic areas. Singapore will focus on building understanding and raising awareness in these areas, as well as conducting training and exercises to raise capacity.

To do so, Singapore will partner the international community, Dialogue Partners and ASEAN Member States (AMS) to organise workshops, seminars and conferences that advance international and regional cooperation in these aspects. We will also support the active role played by the ASEAN Regional Forum (ARF) countries in fostering cyber confidence building and capacity building measures.

Singapore will establish an ASEAN Cyber Capacity Programme from 2017 to complement the various existing ASEAN initiatives.

15th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings

FACILITATE INTERNATIONAL AND REGIONAL EXCHANGES ON CYBER NORMS AND LEGISLATION

GovernmentWare 2015 Conference

Consensus and agreement among nations are key to ensuring the success of cybersecurity cooperation. Singapore aims to be an active participant in this area and will facilitate global and regional dialogues on cyber norms building and codes of conduct, cyber policy and legislation, cyber deterrence and cybercrime cooperation.

For example, the annual RSA Conference Asia Pacific and Japan includes public sector events such as the ASEAN Senior Officials Roundtable on Cybercrime (SORC). The SORC provides a unique platform for high-level discussions among industry leaders and senior government officials from ASEAN and Dialogue Partner countries as well as relevant international organisations. Singapore will host an annual Singapore International Cyber Week (SICW) to catalyse, stimulate and promote exchanges on current and emerging issues pertinent to the cyber community.

The first SICW, to be held in October 2016, will launch the inaugural ASEAN Ministerial Conference on Cybersecurity and the International Cyber Leaders' Symposium as premier regional platforms to discuss key cybersecurity issues facing policymakers. As part of the SICW, the ASEAN Cybercrime Prosecutors' Roundtable Meeting will bring together specialised cybercrime prosecutors from across ASEAN for the first time. The meeting provides an opportunity for cybercrime prosecutors and law enforcement agencies to take stock of the legal capacities of ASEAN. It will also address gaps to raise the overall capabilities in the region. Finally, the SICW incorporates the GovernmentWare conference, which has brought together thought leaders and practitioners to discuss practical cybersecurity issues over the last 25 years.

This Strategy is an initiative of the Cyber Security Agency of Singapore (CSA). CSA was established under the Prime Minister's Office (PMO) and is managed by the Ministry of Communications and Information (MCI).

Over the course of a year, representatives from over 50 government agencies, business and professional associations, private companies and academic institutions were consulted. We are grateful to the associations which have engaged their members, and to the many prominent individuals who have graciously offered guidance and advice. Their valuable feedback served as a basis for this Strategy.

01010011 01100101 01100011 01110101 01110010 01101001 01110100 01111001
01000010 01111001 01000100 01100101 01110011 01101001 01100111 01101110