

April 2009

Infocomm Security Masterplan 2

The Infocomm Security Masterplan 2 (MP2), launched in April 2008, is a five-year roadmap which aims to build upon the achievements of the first Masterplan by enhancing the tenacity of our economy against cyber attacks, thereby boosting the confidence of investors in choosing Singapore as a strategic and secure location for their investments.

Developed through a multi-agency effort led by IDA, under the guidance of the National Infocomm Security Committee, MP2 has the public, private and people sectors working even more closely together to secure Singapore's cyber space. The framework for MP2, as shown in the figure below, depicts the vision, coverage, strategic outcome and the supporting strategic thrusts. Four strategic thrusts have been identified to support MP2's aim of attaining high resilience and availability of the nation's infocomm infrastructure and services:

- Harden national infocomm infrastructure and services
- Enhance infocomm security competencies
- Cultivate vibrant infocomm security ecosystem
- Increase international collaboration



Strategic Thrust 1: Harden national infocomm infrastructure and services

It is vital that Singapore's national infocomm infrastructure and services are "hardened" against emerging threats since they form the foundation layer for

other services and sectors. As such, programmes under this strategic thrust aim to enhance the resilience of our underlying foundation to combat cyber threats.

Strategic Thrust 2: Enhance infocomm security competencies

This strategic thrust looks at enhancing security competencies of infocomm users and infocomm security practitioners. For instance, new programmes are seeking to catalyse greater adoption of essential security practices among infocomm users and ensure that infocomm security practitioners have adequate knowledge and capability in managing infocomm security risks.

Strategic Thrust 3: Cultivate vibrant infocomm security ecosystem

The presence of a vibrant infocomm security ecosystem strengthens Singapore's capability to protect our national infocomm infrastructure and services. An active infocomm security research and development scene is helping to ensure that a variety of up-to-date infocomm security solutions are available to counter constantly evolving infocomm security threats.

Strategic Thrust 4: Increase international collaboration

Given the borderless nature of cyber threats, it is therefore important to continue to work closely with our international counterparts. MP2 also focuses on exchanging best practices in infocomm security, and exploring collaborations in this area.

Highlights of Key MP2 Programmes

Since its launch, the Government is working in close collaboration with the private sector to achieve the outcome of MP2.

I. Association of Information Security Professionals (AISP)

The AISP is a Government and Industry collaboration which aims to transform infocomm security into a distinguished profession and build a critical pool of competent infocomm security professionals who subscribe to the highest professional standards. The first such association in Asia, it hopes to elevate the standing, professionalism and trust accorded to security practitioners here.

Since its formation in April 2008, AISP has achieved considerable progress. For instance, it has now developed a code of conduct and qualifying criteria for their membership. They are currently developing the Infocomm Security Professionals Roadmap and Body of Knowledge with IDA to raise the proficiency of infocomm security professionals in Singapore. Please refer to the factsheet on the **Infocomm Security Professionals Roadmap and Body of Knowledge** for further information.

II. National Infocomm Scholarship for Infocomm Security

The National Infocomm Scholarship (NIS) for Infocomm Security was announced in April 2008. With the growing pervasiveness of infocomm technology use by the Government, businesses and society, there is a need to ensure a continuous pipeline of competent infocomm security professionals. Moreover, in order for infocomm security to flourish in Singapore, there is also a need to ensure that talents are attracted to join this profession.

In partnership with the public and private sector organisations listed in **Annex A**, scholarships will be offered to top students who wish to specialise in infocomm security. The scholarships will lead to Bachelor and Master degrees in infocomm security. The first batch of NIS – Infocomm Security Scholarships will be awarded in August 2009.

The scholarship, available to both local and foreign students, is open to those who have completed their junior college or polytechnic studies and are keen to pursue a full time infocomm-security related degree in either a local or foreign university of their choice. Interested students can apply for this scholarship at www.talent.singaporeinfocomm.sg. The application period is from January to March every year.

III. Cyber Security Awareness Alliance

Besides focusing on the development of infocomm security professionals, there is also a need to raise the awareness and adoption of essential cyber-security practices among users. In the security value chain, the human factor is often seen as the last line of defence against cyber attacks. To this end, the IDA and like-minded partners from the public and private sectors formed the Cyber Security Awareness Alliance (Alliance) in 2008. See **Annex B** for a list of participating organisations in the Alliance.

As a collaborative body, the Alliance will amalgamate efforts from its members by bringing together different strengths and resources. The aims of the Alliance are to:

- (i) Build a positive culture of cyber security in Singapore, and
- (ii) Promote and enhance awareness and adoption of essential cyber security practices for the people and private sectors.

In the past year, the Alliance has consolidated its resources to raise the level of cyber security awareness through media outreach and conferences/workshops. For example, articles contributed by alliance partners focusing on security for SMEs were published in the Business Times.

Various conferences and workshops were also conducted to target different audiences. For example, a Cyber Security Wellness Workshop targeted at heart-landers was organised by the Singapore Police Force, with the participation of other alliance partners. Similarly, the Singapore Chinese

Chamber of Commerce and Industry's Annual Conference and the Youth Infocomm Day were leveraged to reach out to SMEs and students.

As cyber threats evolve, plans to promote and enhance awareness and adoption of essential cyber security practices continue to be developed.

IV. Sector-Specific Infocomm Security Programme

As each sector has its unique security requirements, a 'one-size-fits-all' approach, where a single solution is developed to meet the needs of different sectors will be insufficient. Sector-specific infocomm security programmes ensure that the infocomm infrastructure and services in each sector remain secure.

The Infocomm sector is a key sector in Singapore. Singapore is one of the most wired nations in the world. Such reliance on the Internet will continue to increase with the implementation of iN2015. Even as Singapore grows in our reliance on the Internet, the risk posed by cyber attacks also grows in sophistication. It is thus crucial to establish sufficient infocomm security measures against prevalent and emergent cyber threats and further enhance the security situational awareness of Singapore's Internet infrastructure.

While Singapore's Internet Service Providers (ISPs) are already paying attention to security issues, IDA is strengthening our engagement with ISPs to further secure our Internet infrastructure to co-create sustainable infocomm security measures that ISPs can implement.

The Government sector is another key sector in Singapore. The Singapore Government is recognised as a global leader in the use of infocomm technology. Through the innovative use of infocomm, it is now more convenient for citizens to interact and transact with the government. Infocomm has also helped our government agencies to operate more efficiently.

Such widespread use of infocomm technology has also opened us to the threats in the cyber world. Over the years, the Government has put in place various infocomm security initiatives to address cyber threat prevention, detection and recovery. As the Government, citizens and businesses become more dependent on infocomm technology, there is a need to continuously reinforce the security and resilience of our government systems and services.

More timely and effective analysis of data from the various security initiatives in the Government is being established. Through such analysis, it is possible to further enhance the security situational awareness across the Government. Trends identified will also help us determine appropriate security measures and programmes to put in place. New initiatives to mitigate emerging threats affecting availability of government systems and services will also be implemented.

V. International Collaboration

The Government continues to actively engage other countries and contribute to global efforts in combating cyber threats. In October 2008, Singapore hosted the Meridian Conference. The annual Meridian Conference is a major programme of the international Meridian Process, which aims to:

- (i) Build trust and establish international relations with senior government policy makers for Critical Information Infrastructure Protection (CIIP),
- (ii) Share strategic approaches and experiences in CIIP from around the world, and
- (iii) Explore benefits and opportunities for cooperation between governments.

The Meridian Process provides Governments worldwide with a means by which they can discuss how to work together at the policy level on CIIP.

At the Conference, Singapore also assumed the Presidency of the Meridian Process. As the President, Singapore is leading a Working Group on cross-border collaboration on CIIP that includes developing a Self-Assessment Scorecard on CIIP and a Reference Repository on International CIIP Collaboration. Members of the working group include Australia, Japan, the Netherlands, UK, USA and the International Telecommunication Union.

There are also other engagements to champion Singapore's commitment to the international community on cyber security. This is achieved through regular exchange of information and experiences with international counterparts – between Governments and between CERTS. Besides bilateral collaborations, sharing and cooperation on a community basis is also important. Examples of established infocomm security fora in ASEAN and Asia-Pacific are ASEAN TELMIN¹ and APCERT² respectively.

¹ The ASEAN Telecommunications and IT Ministers' Meeting (TELMIN) was formed with the aim of fostering stronger regional ties among the telecommunications community in ASEAN. TELMIN meets once a year during which the Ministers hold a dialogue among themselves. Part of the TELMIN annual programme also includes sessions with ASEAN Dialogue Partners of ASEAN, namely, the People's Republic of China, Japan, the Republic of Korea, and India.

² APCERT was established in 2002 and aims to encourage and support the cooperation between national CERTS in the Asia Pacific region. It maintains a trusted network of computer security experts in the Asia Pacific region to improve the region's awareness and competency in relation to computer security incidents. Singapore is a founding member of APCERT (Japan, Malaysia, Australia, South Korea etc) and has been on its Steering Committee since 2002. Currently, Singapore is the deputy chair of the APCERT Steering Committee.

ANNEX A

Organisations currently participating in the National Infocomm Scholarship:
Infocomm Security:

	Organisation
1.	BT Frontline Pte Ltd
2.	Centre for Strategic Infocomm Technologies
3.	e-Cop Pte Ltd
4.	Singapore Power Ltd
5.	Singapore Telecommunications Ltd
6.	Infocomm Development Authority of Singapore
7.	Symantec Singapore Pte Ltd

ANNEX B

Organisations represented on the Cyber Security Awareness Alliance:

	Organisation
1.	Association of Small and Medium Enterprises
2.	BT Frontline Pte Ltd
3.	Cisco Systems (USA) Pte Ltd
4.	eBay Southeast Asia
5.	Hewlett-Packard Singapore (Sales) Pte Ltd
6.	Infocomm Development Authority of Singapore
7.	Juniper Networks (Singapore) Pte Ltd
8.	McAfee (Singapore) Pte Ltd
9.	Microsoft Singapore Pte Ltd
10.	National Crime Prevention Council
11.	Quantiq International Pte Ltd
12.	Singapore Business Federation
13.	Singapore Chinese Chamber of Commerce & Industry
14.	Singapore Infocomm Technology Federation
15.	Singapore Police Force
16.	Symantec Singapore Pte Ltd

FOR MORE INFORMATION

IDA Communication Contact: Ms Tan Sock Gim, Manager, Tel:+65 6211 1350, E-mail: Tan_Sock_Gim@ida.gov.sg