
NATIONAL
CYBER
SECURITY
MASTERPLAN
2018
iDA
INFOCOMM
DEVELOPMENT
AUTHORITY OF
SINGAPORE

CONTENTS

INTRODUCTION

The cyber landscape evolves rapidly, and so too must Singapore's efforts to foster a secure and resilient national infocomm environment.

With infocomm technologies playing an increasing role in enhancing key economic sectors and building a well-connected society, the importance of a comprehensive masterplan cannot be overstated.

Since 2005, infocomm security masterplans have provided Singapore with strategic directions in securing its infocomm environment, while taking a balanced approach between security requirements and ease of conducting business or daily activities. The National Cyber Security Masterplan 2018 (NCSM2018) is the latest five-year plan to enhance the cyber security of Singapore's public, private and people sectors. In addition to Government and Critical Infocomm Infrastructure (CII), its scope has now been broadened to take into consideration businesses and individuals.

Under the guidance of the National Infocomm Security Committee (NISC), and led by IDA, its Whole-of-Government approach aligns the efforts of multiple government agencies in strengthening resilience against cyber threats. This will help Singapore realise the vision of becoming a **Trusted and Robust Infocomm Hub**.

BRIEF HISTORY OF THE MASTERPLANS

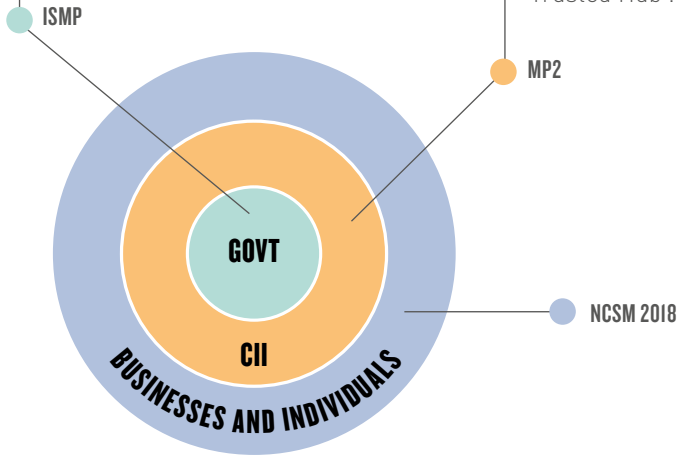
Singapore's Infocomm Security Masterplans are reviewed every 3 – 5 years. This ensures that Singapore continues to be a secure and trusted infocomm environment, capable of mitigating cyber threats and meeting long-term societal and economic needs.

INFOCOMM SECURITY MASTERPLAN (2005-2007)

The first Infocomm Security Masterplan (ISMP) initiated Singapore's concerted efforts towards a secured infocomm environment by first making the Government's infocomm environment more secure.

INFOCOMM SECURITY MASTERPLAN 2 (2008-2012)

In 2008, the ISMP was succeeded by a second Masterplan (MP2), a five-year roadmap that built upon the achievements of its predecessor and expanded coverage to include Critical Infocomm Infrastructure (CII) to make Singapore a 'Secure and Trusted Hub'.



NATIONAL CYBER SECURITY MASTERPLAN 2018

Focus group discussions were held with companies such as Microsoft, Symantec, McAfee and associations such as SITF, AISP, (ISC)2 to identify the strategic directions for NCSM2018

The National Cyber Security Masterplan (NCSM2018) builds on the work undertaken in the earlier masterplans. It seeks to bring Singapore's infocomm security to the next level of maturity and sophistication. In addition to Government and CII, the NCSM2018 will expand its scope to cover the **wider infocomm ecosystem, including businesses and individuals**.

In order to craft a holistic strategy, IDA conducted extensive consultation and gathered feedback from the industry through numerous avenues, such as focus group discussions and IDA's annual Business Infocomm Usage Survey. In total, over 60 agencies, local enterprises and industry associations were consulted for ideas and input for the masterplan. From the feedback, strategic drivers were identified which served as the basis for NCSM2018.

STRATEGIC DRIVERS

RISING SOPHISTICATION OF CYBER THREATS

With an ever-increasing number of threats and adversaries, the cyber environment is a volatile one. The advancements in ICT have also created more pathways for malicious actors to exploit.

The malware industry continues to thrive. In Q1 2014 alone, McAfee reported more than 30 million new malware samples in their database. In addition, Distributed Denial of Service (DDoS) attacks continue to disrupt organisations and businesses. In March 2013, anti-spamming organisation Spamhaus was hit by one of the biggest DDoS attacks thus far, peaking at 300 Gigabits per second.

Cyber attacks have also become more sophisticated, with social engineering[1] and spear phishing[2] attacks becoming commonplace. According to the Symantec Internet Security Threat Report, an average of 83 spear phishing attacks occurred each day globally in 2013.

An even greater menace has arrived in the form of Advanced Persistent Threats (APTs)[3], featuring highly sophisticated and targeted malware such as Stuxnet and Duqu. APTs can circumvent typical cyber security measures and have compromised organisations thought to be better equipped to defend against them, such as network security company RSA and defence contractor Lockheed Martin.

[1] Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.

[2] Spear Phishing is a way of attempting to acquire information by masquerading as a trustworthy source in an electronic communication.

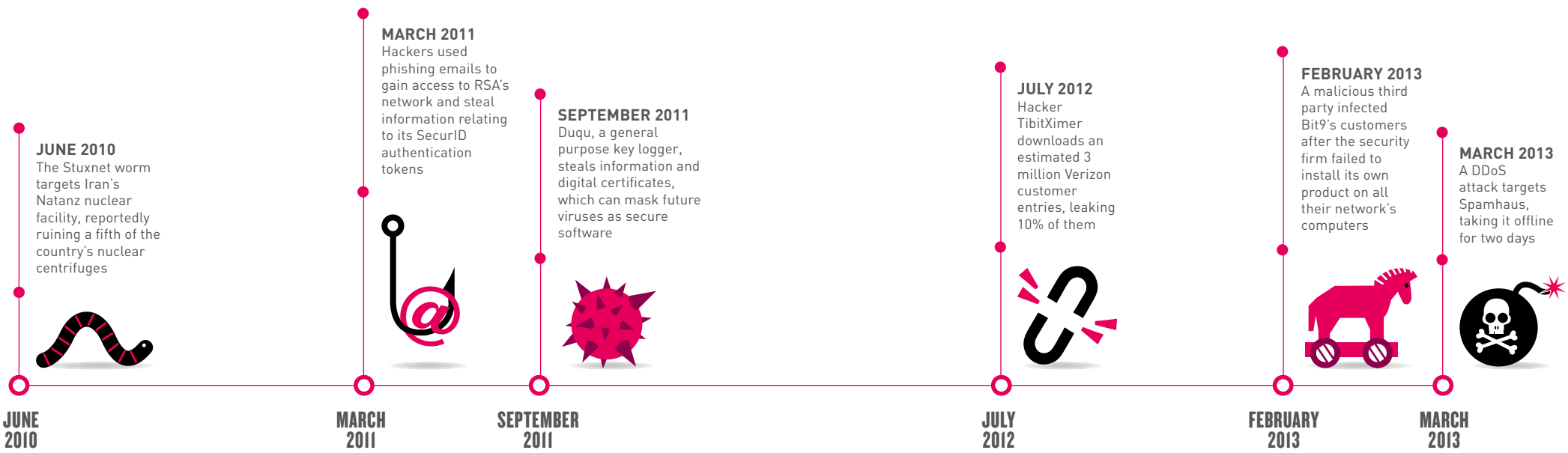
[3] An advanced persistent threat (APT) is a targeted attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.

SUPPLY CHAIN AS CONDUITS TO ATTACK HIGH VALUE TARGETS

Cyber security is only as strong as its weakest link. Increasingly, small and medium-sized enterprises (SMEs) are being exploited and used as conduits to attack higher-value targets in their supply chain.

A 2013 report by Symantec revealed that 41% of targeted attacks were aimed at small companies, more than double the number in 2011. The 2012 Verizon Data Breach Investigations report also found that a majority of the 855 data breaches it had analysed targeted smaller firms. In 2012, Verizon itself made headlines when a hacker stole and posted 300,000 of its customer records on the Internet. The data had been stolen from a third-party marketing firm that Verizon used. In Singapore, it was reported in December 2013 that information belonging to nearly 650 private banking customers were stolen after the vendor contracted by the bank to print statements was hacked.

Another form of supply chain hacking was to attack the firms providing protection, such as the March 2011 attack on RSA that was subsequently used to infiltrate the Virtual Private Networks of American defence company Lockheed Martin. In February 2013, security firm Bit9 was similarly hacked and its encryption keys were used to send malware to its clients, among which included the U.S. government and at least 30 Fortune 100 firms. Supply chains thus represent an extension of the attack surface of high value targets.



CHANGING INFOCOMM TECHNOLOGY ENVIRONMENT

The growth of mobile infocomm technology has created a paradigm shift in how people engage with digital information. Many users are now used to accessing data and infocomm services anywhere, anytime. This has spurred the adoption of Bring-Your-Own-Device (BYOD)[4] policies by businesses and organisations. Mobile malware has also risen substantially as hackers turn their attention towards the increasing number of mobile device users.

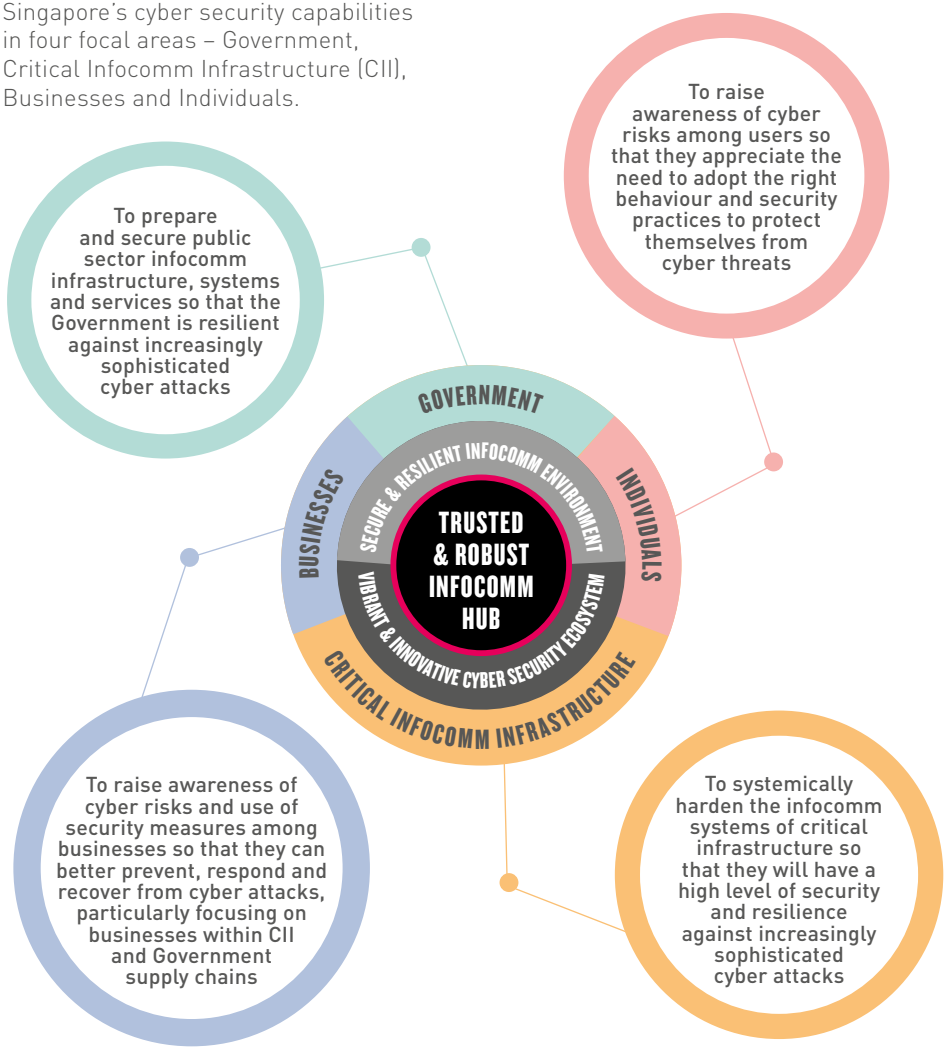
At the same time, the way in which infocomm services are delivered has also changed. Organisations are increasingly leveraging on cloud computing technology and shared services. With the global Cloud services market experiencing growth from US$93 billion in 2011 to US$110 billion in 2012, and potentially up to US$210 billion in 2016, we can only expect greater exposure of our information assets to risks posed by the Internet.

Singapore's security measures must thus evolve and keep pace with the changing infocomm environment. Guided by NCSM2018, the government will work closely with the private and people sectors, further upgrading and strengthening cyber security capabilities to ensure that Singapore will be able to deal with cyber threats effectively.

[4] Bring Your Own Devices (BYOD) is the practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for work purposes.

FOCAL AREAS – GOVERNMENT, CII, BUSINESSES AND INDIVIDUALS

The NCSM2018's mission is to enhance Singapore's cyber security capabilities in four focal areas – Government, Critical Infocomm Infrastructure (CII), Businesses and Individuals.

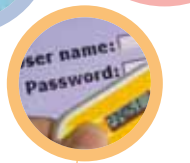


KEY ENABLERS - MANPOWER, INDUSTRY, R&D, DOMESTIC/ INTERNATIONAL COLLABORATION

To achieve the outcomes mentioned in the focal areas, the following key enablers will be implemented:

INCREASE DOMESTIC AND INTERNATIONAL COLLABORATION:
To ensure co-ordinated action against cyber threats

DEVELOP HUMAN CAPITAL:
To enlarge the pool of experts with sophisticated infocomm security skills and provide more facilities to sharpen their skills



CULTIVATE RESEARCH & DEVELOPMENT:
To cultivate innovative and forward-looking infocomm security research and development capabilities

CATALYSE INDUSTRY DEVELOPMENT:
To ensure up-to-date infocomm security solutions are available to Government, businesses and individuals

KEY STRATEGIC IMPERATIVES

To realise the NCSM2018 vision of Singapore becoming a Trusted and Robust Secure Infocomm Hub by 2018, three key strategic imperatives have been identified.

ENHANCE SECURITY AND RESILIENCE OF CII TO DEAL WITH SOPHISTICATED ATTACKS

New and sophisticated threats, such as APTs, complicate the task of prevention. Hence, there is a need to enhance the security and resilience of CII to deal with such sophisticated attacks.

CRITICAL INFOCOMM INFRASTRUCTURE

As part of the continuous efforts to enhance the protection of critical infocomm infrastructure (CII) and improve cross-sector response to mitigate widespread cyber attacks, the Government works closely with critical sectors on cyber security exercises, as well as to assess critical infrastructure for vulnerabilities and ensure that security capabilities and measures are in place to mitigate cyber threats.

The **Critical Infocomm Infrastructure (CII) Protection Assessment programme** assesses the security of infocomm systems that are critical to the operation of CII in Singapore, ensuring that CIIs remain secure and resilient.

The **Critical Infocomm Infrastructure Security Assessment (CII-SA)** appraises the infocomm security readiness of Singapore's Critical Infocomm Infrastructure (CII) and ascertains the adequacy of infocomm protection measures, implemented by infrastructure owners and operators.

The **Secure and Resilient Internet Infrastructure Code of Practice (SRII-CoP)**, aligned with international standards and best practices, has been issued by IDA to designated ISPs. The Code of Practice has been incorporated into the telecommunications regulatory framework and sets specific security controls and outcomes to ensure that essential security is maintained to mitigate current and emerging cyber threats. Periodic audits are conducted by IDA to ensure that ISPs observe the Code of Practice.

The **National Cyber Security Exercise programme** uses exercises to assess the capability and readiness of critical sectors, aiming to improve the overall resilience of our national infrastructure and services to significant cyber attacks at the national level.

GOVERNMENT

As part of the continuous efforts to enhance the security and resilience of its infocomm infrastructure, and public sector capabilities, the Government will focus on proactive defence-in-depth to mitigate increasingly sophisticated attacks. These include upgrading of existing detection and analysis capabilities and strengthening preventive and recovery measures at the Whole-of-Government level.

The **enhanced Cyber Watch Centre (CWC)** will leverage on advanced tools and techniques, better detection and correlation to improve the overall effectiveness of security monitoring for the public sector.

The **enhanced Threat Analysis Centre (TAC)** will utilise state-of-the-art analytical tools to assess larger volumes of data from a wider range of sources, to provide public agencies with detailed cyber threat analysis, advisories and recommendations so that they can take timely preventive actions.

INCREASE EFFORTS TO PROMOTE ADOPTION OF INFOCOMM SECURITY MEASURES AMONG INDIVIDUALS AND BUSINESSES

Due to the inter-connectivity forged through infocomm technologies, cyber attacks could potentially ripple beyond the immediate victims amongst businesses and individuals given their roles as supply chain and employees respectively.

SMEs and individuals are perceived to have weaker capabilities and lower resistance to cyber attacks. This is of particular concern as SMEs comprise 99% of all enterprises in Singapore, as at Aug 2014. As such, current efforts will be reinforced to raise infocomm security awareness and adoption among businesses and individuals.

The **Cyber Security Awareness and Outreach programme** aims to augment existing outreach channels and explore new avenues that offer wider coverage and reach to users, such as broadcast media.

For example, cyber security awareness videos in both English and Mandarin could be uploaded onto popular video sharing websites. Winning videos from the National Infocomm Security Competition's Multimedia Design segment will also be shown on local television channels to promote cyber security best practices. Cybercrime cases will be featured in Crimewatch, a regular public education television programme that re-enacts real-life crime cases. This will give viewers a better understanding of cyber threats such as identity theft and social engineering and encourage them to adopt safe online practices.

In addition, the NCSM2018 will also include initiatives to facilitate information sharing between the Government and private sector, as well as collaborations with industry and trade associations to promote cyber security. Information such as security advisories and threat information can be shared to enhance businesses' ability to assess risks, make security investments and take protective actions.

GROW SINGAPORE'S POOL OF INFOCOMM SECURITY EXPERTS

The threat posed by increasingly sophisticated cyber attacks is exacerbated by a shortage of highly skilled defenders. This shortage is not unique to Singapore. More than half (56%) of the respondents in the 2013 Global Information Security Workforce Study (GISWS) indicated that their security functions were short-staffed.

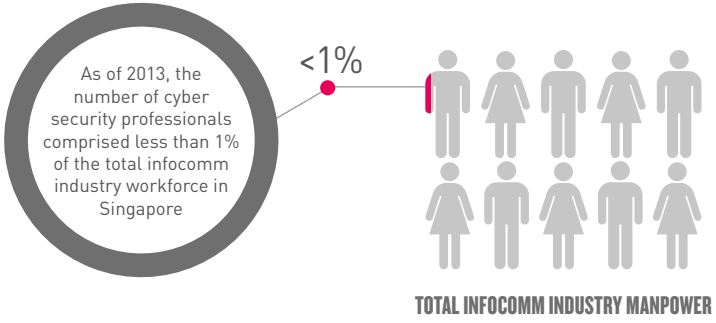
There is a pressing need to explore new initiatives to boost the numbers and skill levels of cyber security professionals, as well as to retain them in Singapore.

To alleviate this situation, the NCSM2018 will push further to develop human and intellectual capital within Singapore's infocomm industry.

PROMOTION OF R&D TO ATTRACT AND CULTIVATE MORE CYBER SECURITY EXPERTISE

The **National Cybersecurity R&D Programme** seeks to develop R&D expertise in cyber security and improve cyber infrastructure with an emphasis on security, reliability, resiliency and usability. The programme, involving NRF, MINDEF, MHA, NSCS, IDA and EDB, aims to promote collaboration among agencies, academia, research institutes and private sector.

A 5-year S$130 million fund has been committed to support research efforts into both technological and human-science aspects of cyber security, complemented by studies into cyberspace governance and policy research.



TRAINING PROGRAMME TO DEVELOP INFOCOMM SECURITY SPECIALISTS

The **Company-Led Training (CLT) Programme** for Fresh Professionals is an initiative by IDA, in collaboration with CLT Partners. CLT aims to recruit, mentor and train fresh professionals in areas and technologies relevant to the local infocomm industry, including Software Security Administration, which is essential to an organisation's cyber security.

Currently, various infocomm security companies provide in-house training for entrant-level professionals, and some have indicated a willingness to train these professionals beyond their own needs. CLT thus aims to fast-track fresh infocomm security professionals toward specialist-level jobs.

Trainees will receive fundamental training in infocomm security in the CLT Partner's business unit. This offers them the opportunity to apply what they have learned and recommend solutions in live projects. Feedback will be provided by mentors and the training duration will span up to a year.

CYBER TRAINING FACILITY FOR TESTING / TRAINING OF CYBER SECURITY EXPERTS

The **DigiSAFE Cyber Security Centre**, officially opened in June 2014, offers highly sophisticated operations-centric cyber security training that better prepares cyber security professionals in detecting and responding to cyber attacks. The Centre's training programmes allow trainees to experience realistic simulations of real-world malicious attacks.

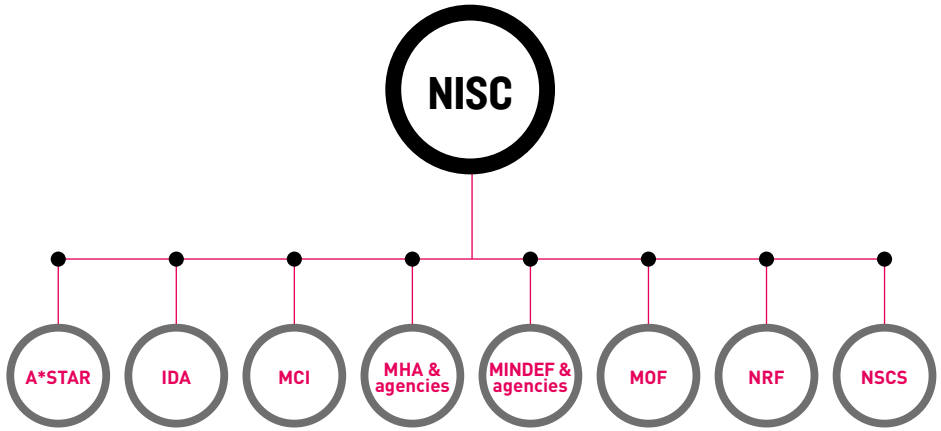
STRATEGIC COLLABORATIONS

The importance of a collaborative approach towards cyber security cannot be overstated, as it enables the pooling and sharing of resources and knowledge across different entities to achieve greater synergy and more refined solutions. In Singapore, domestic collaboration spanning across government agencies, and between the government and private sector, is complemented by conscientious efforts to engage other countries in international collaborations.

NATIONAL-LEVEL COMMITTEE

The **National Infocomm Security Committee (NISC)** comprises of senior leadership from multiple government agencies including the Agency for Science, Technology and Research (A*STAR), Infocomm Development Authority of Singapore (IDA), Ministry of Communications and Information (MCI), Ministry of Home Affairs (MHA) and its agencies, Ministry of Defence MINDEF) and its agencies, Ministry of Finance (MOF), National Security Coordination Secretariat (NSCS) and National Research Foundation (NRF). Besides being the national platform that formulates infocomm security policies and sets strategic directions for Singapore, NISC also guides the development and implementation of the NCSM2018.

The multi-agency committee takes a risk-based approach to cyber security, balancing the advantages of using new technologies and capabilities against the related security risks. While recognising that infocomm technology and the Internet can enhance service quality and create new opportunities, these technologies can also potentially be exploited for malicious activities such as data or identity theft that will significantly impact businesses.



PUBLIC-PRIVATE PARTNERSHIPS

CYBER SECURITY AWARENESS ALLIANCE

The Cyber Security Awareness Alliance was formed in 2008 by IDA and other like-minded partners from the Government, private enterprises, trade associations and non-profit organisations. The Alliance amalgamates the efforts of its members by utilising their collective resources and bringing together different strengths. It aims to:

- Build a positive culture in Singapore where cyber security becomes second nature to all infocomm users; and
- Promote and enhance awareness and adoption of essential infocomm security practices for the private and people sectors

Over the years, the Alliance had been reaching out to the People and Private sectors through exhibitions, talks, as well as flagship events to promote awareness and adoption of essential security measures. Some of its key flagship events are:

The **Cyber Security Awareness Campaign** has been held annually since 2011 to reinforce security awareness messages to Government, business and individual users. Through the years, the Campaign has in turn focused on Computer Security, Mobile Security, Wireless Security and Online Security. From 2011 to 2013, the Campaign prompted an average of 600,000 pledges per year by businesses and individuals responding to the call-to-actions to secure their computers, wireless equipment, mobile devices and online identities. Advertisements were also placed in national newspapers such as The Straits Times, TODAY and MyPaper. In addition, exhibitions, roadshows and talks were held at public locations such as libraries and residential hubs to promote the call-to-actions.

gosafeonline.sg
Cyber Security Awareness Alliance

The **National Infocomm Security Competition (NISEC)**, a feature of the Cyber Security Awareness Campaign since 2013, aims to educate the public about cyber security and the need to adopt simple yet secure online practices. NISEC engages the younger generations, ranging from primary to tertiary levels, in competitions such as poster design, model design, multimedia video creation, secure coding and penetration of web applications.

The Alliance maintains a web portal https://www.gosafeonline.sg to promote and inculcate safe infocomm practices for the public, private and people sectors. The Alliance also leverages on popular social media and networking websites to connect with its target audience.

For the rising numbers of mobile device users, the Alliance is planning to launch a mobile application for Android and iOS platforms. Some of the features include:

- Events Calendar
  Lists Infocomm Security Events that will be held in Singapore
- Security News
  Features the latest infocomm security-related news and articles from Go Safe Online Portal
- Security Alerts
  Updates users on security vulnerabilities for commonly used software
- Password Checker
  Allows users to verify the strength of their passwords and set reminders for periodic changing of passwords

ASSOCIATION OF INFOCOMM SECURITY PROFESSIONALS (AISP)

The Association of Infocomm Security Professionals (AISP), a collaboration between Government and Industry, aims to uplift 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 of such associations in Asia, the AISP plans to:

- Promote, develop, support and enhance the integrity, technical competence, management expertise, status and interests of information security professionals in Singapore
- Promote the development, increase and spread of information security knowledge and of any related subject

AMBIENT NETWORKS SECURE ECO SYSTEM

The Ambient Network Secure Eco System (ANSES) is an initiative to enhance the secure interoperability of pervasively deployed "smart" devices in large networks. One outcome of the initiative is the development of a security framework and standards compliance for IT security hardening and attack protection for mobile devices, embedded systems and SCADA systems. Products developed include a secure and encrypted USB flash storage solution for mobile workers named Secure USB for Roaming Users (SURU), and a Secure Printing System to send print jobs securely over a network. To foster public-private partnership and collaboration, a series of outreach events known as "ANSES RahRah seminars" were also held on a quarterly basis to share ideas and showcase solutions to industry players, academia and the public and private sectors.

INTERNATIONAL COLLABORATIONS

The Singapore Government continues to engage other countries and contribute to global efforts in combating cyber threats. Some of these engagements include:

ASEAN TELMIN

The ASEAN Telecommunications and IT Ministers' Meeting (TELMIN) was established in 2001 to serve as the main regional platform to discuss and enhance cooperation and collaboration among ASEAN member states. Held annually to discuss the key focus and direction of regional cooperation, TELMIN also aims to strengthen cooperation with ASEAN Dialogue Partners such as the People's Republic of China, Japan and the Republic of Korea.

Singapore contributes actively to the TELMIN and its various sub-meetings to make ICT an engine of growth for ASEAN and to support the building of an ASEAN community. A key contribution from Singapore is the building of confidence and trust in network and information security infrastructure to further promote trade and the use of ICT, as well as to protect the flow of information. This is done through various activities such as the ASEAN Network Security Action Council (ANSAC), ASEAN-Japan Information Security Policy Meeting and the ASEAN CERT Incident Drill (ACID).

ASEAN-JAPAN ANNUAL ENGAGEMENTS

Singapore is an active participant in ASEAN-Japan engagements that range from awareness and outreach, policy research, information sharing to operational co-operation among CERTs/CSIRTs. These engagements are anchored by two annual events, namely the **ASEAN-Japan Information Security Policy Meeting** and the **ASEAN-Japan Government Network Security Workshop** that Singapore participates in. The Policy Meeting is the platform for deliberation on strategic issues while the Workshop is primarily used to discuss initiatives for collaborations such as the annual Cyber Security Awareness Month.

Singapore is a member of the **Proactive Response Against Cyber-attacks Through International Collaborative Exchange (PRACTICE) project**, led by the Ministry of Internal Affairs and Communications of Japan, that is trying to establish a global monitoring and analysis framework to protect users from malware infection and malicious activities in cyberspace.

Other Japan-led initiatives included the Tsubame project, an Internet threat monitoring system, and the annual Communications Check Exercises to build closer relationship between ASEAN member states and Japan as well as establish more effective information sharing processes to aid decision-making for policy makers. SingCERT represents Singapore in both initiatives.

In 2013 and 2014, SingCERT also participated in a Japan-led Communications Check Exercise, which aims to build better relationships between ASEAN member states and Japan, and establish more effective information sharing processes to aid in decision-making for policy makers.

ASIA PACIFIC CERT (APCERT)

APCERT was established to encourage and support the cooperation between national CERTs in the Asia Pacific region by maintaining a trusted network of computer security experts in the region who can collectively improve the region's awareness and competency in relation to computer security incidents. Singapore is one of the founding members of the APCERT and participates actively in the annual **APCERT AGM & Conference** and **APCERT Cyber Drill**. The APCERT AGM aims to create a safe, clean and reliable cyber space in the Asia Pacific region. The APCERT Cyber Drills involve global coordination to conduct drills including CII protection, APT mitigation and mitigation of large scale DoS attacks.

ASEAN CERT INCIDENT DRILL (ACID)

SingCERT actively promotes collaboration among the CERTs in ASEAN. For example, SingCERT developed the "Minimum Performance Guideline for Setting up of a National CERT" and "Guidelines on Information Sharing". Both documents have been accepted by ASEAN as reference materials for all members.

Since 2006, SingCERT plans and runs ACID on an annual basis. This drill is meant to strengthen cooperation among CERTs of ASEAN members and dialogue partners, and test the points of contact in each incident response team and their incident handling procedures.

FIRST (FORUM OF INCIDENT RESPONSE AND SECURITY TEAM)

FIRST is an international confederation of trusted computer incident response teams who cooperate to handle computer security incidents and promote incident prevention programmes.

- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organisations from around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment.

SingCERT is one of the participating teams in FIRST.

MERIDIAN PROCESS

Singapore is a regular participant in the annual Meridian Conference. The conference is a major programme of the international Meridian Process, which aims to:

- Build trust and establish international relations with senior government policy makers for Critical Information Infrastructure Protection (CIIP)
- Share strategic approaches and experiences in CIIP from around the world
- 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.

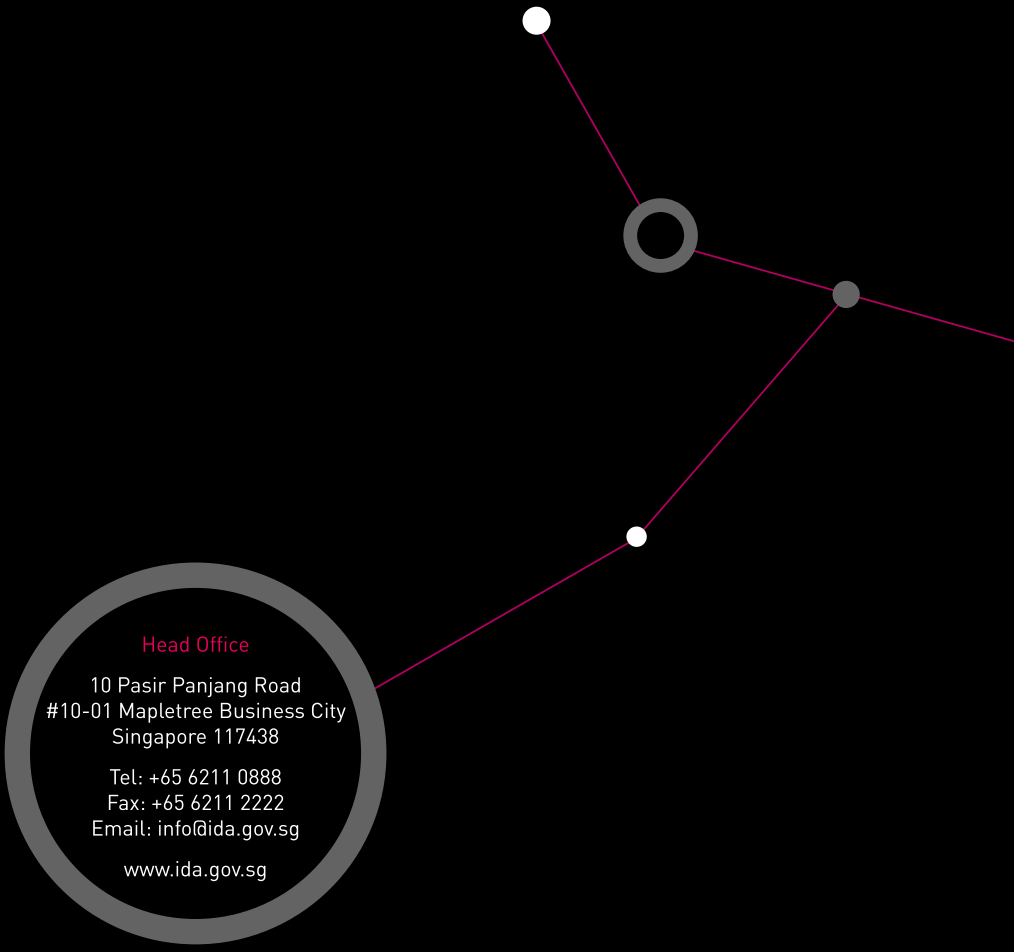
CONCLUSION

The Infocomm Security Masterplans will continue to serve as strategic blueprints to guide Singapore's efforts to foster a secure and resilient national infocomm environment, while taking a balanced approach between security requirements and ease of conducting business or daily activities.

With cyber threats expected to become ever more sophisticated, it is vital for the Government, businesses and individuals to exercise vigilance and continually strengthen Singapore's infocomm infrastructure and systems.

Our nation's resilience against cyber threats will also appeal to investors by boosting their confidence in selecting Singapore as a strategic and secure location for their investments.

Given our heavy reliance on infocomm, Singapore needs to build up our pool of infocomm security professionals and develop their competencies. Only then can we better mitigate cyber threats and provide a trusted and secure online environment for businesses and individuals.



Head Office

10 Pasir Panjang Road
#10-01 Mapletree Business City
Singapore 117438

Tel: +65 6211 0888
Fax: +65 6211 2222
Email: info@ida.gov.sg

www.ida.gov.sg