THE SINGAPORE CYBERSECURITY STRATEGY

2021

Acknowledgements

We would like to thank the following individuals, groups, and agencies for their valuable input and support over the course of developing the Singapore Cybersecurity Strategy 2021:

- Dr Benjamin Ang, Centre of Excellence for National Security, S. Rajaratnam School of International Studies
- Mr Bruce W. McConnell, EastWest Institute
- Prof Ciaran Martin, Blavatnik School of Government, University of Oxford
- Mr Christopher C. Krebs, Krebs Stamos Group
- Mr Christopher Painter, Global Commission on the Stability of Cyberspace
- Mr James Andrew Lewis, Center for Strategic & International Studies
- Dr Shashi Jayakumar, Centre of Excellence for National Security, S. Rajaratnam School of International Studies
- The Singapore Cyber Security Inter Association
- The Cyber Security Awareness Alliance
- The Infocomm Media Development Authority
- The Ministry of Communications and Information
- The Ministry of Defence
- The Ministry of Home Affairs
- The Personal Data Protection Commission
- The Singapore Police Force
- The Smart Nation and Digital Government Group

The Singapore Cybersecurity Strategy 2021
Copyright © 2021
by Cyber Security Agency of Singapore
All rights reserved.

ISBN: 978-981-18-2258-2

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

Designed by:
APT811 Design & Innovation Agency
www.apt811.com

PRIME MINISTER'S FOREWORD

Five years ago, we launched the first Singapore Cybersecurity Strategy. The world is now a different place. Digital technology has transformed how we live, work, and play. Smart homes and devices are becoming mainstream; retail stalls are pitching their wares over livestreaming apps; we PayNow each other instead of using cash. The COVID-19 pandemic has accelerated these trends further.

Digital technology is central to our COVID-19 response. Technology enables us to trace contacts effectively and efficiently, monitor patients' health remotely, and ensure compliance with stay-at-home notices. Many solutions were developed locally to help us emerge stronger from the pandemic.

Singapore must continue to exploit digital technology fully to grow and develop. At the same time, we must be vigilant about the risks. The more we digitalise, the more exposed we become to the growing threats in cyberspace. The same technologies that improve our lives can be misused to disrupt our lives, sow mistrust, and deepen social divisions. Cyberattacks can also do physical damage to business operations and essential infrastructure, and pose real-world threats to lives and livelihoods.

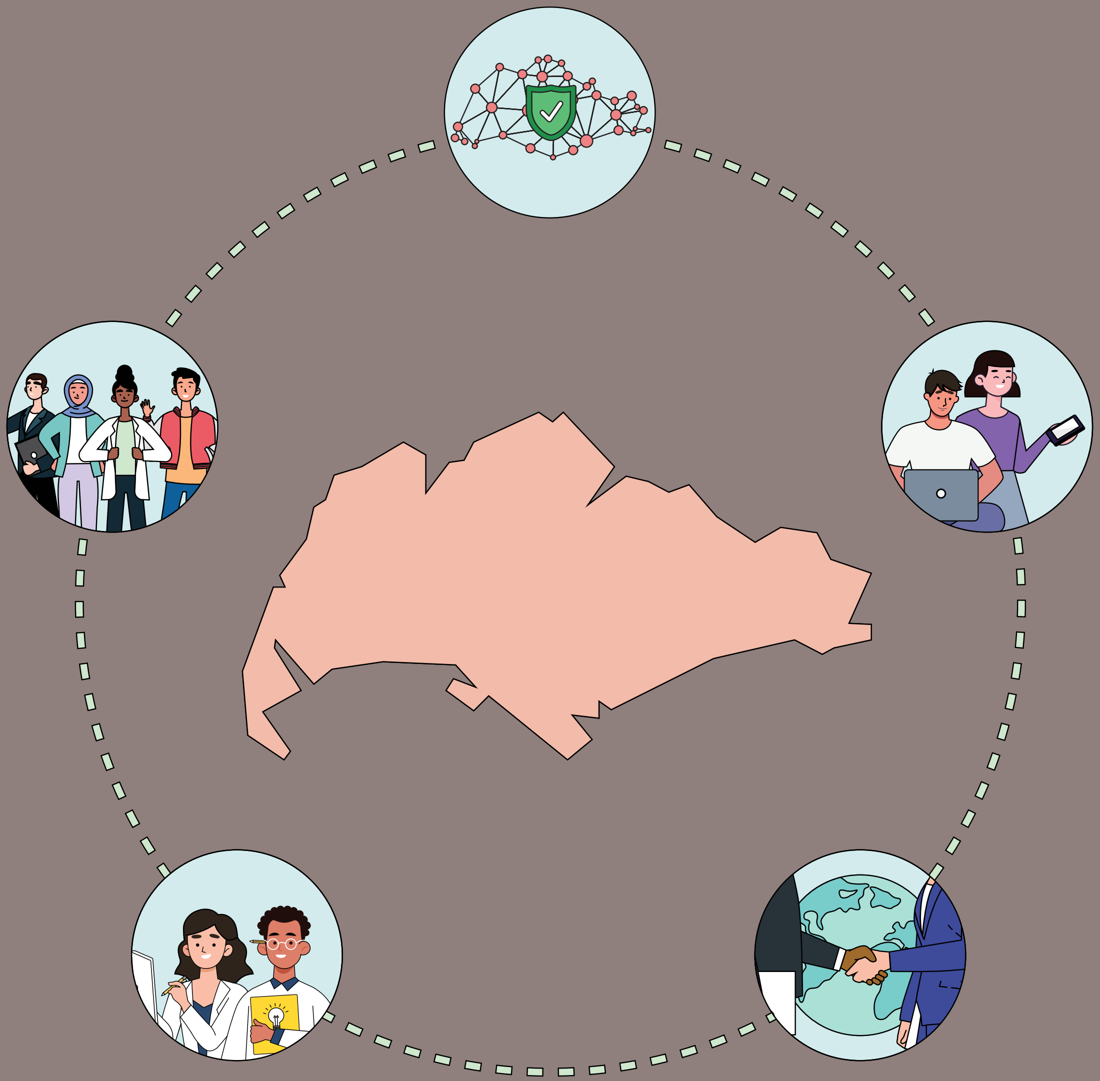
Digitalisation and cybersecurity are thus two sides of the same coin. As we push for digitalisation, we must also raise our cybersecurity levels to protect ourselves from new technological exploits and malicious actors.

This updated Cybersecurity Strategy charts the next stage in Singapore's journey to becoming a more cyber-resilient nation. We will actively defend our cyberspace, simplify cybersecurity for end-users, and promote the development of international cyber norms and standards. As the cyber environment is evolving rapidly, implementing this strategy will demand much of our people. That is why we are investing heavily to upskill practising professionals and to support individuals keen on pursuing a cybersecurity career. If we can do all this well, we can confidently unleash our full digital potential.

As the world rides the digitalisation wave, let us work together towards a trusted and resilient cyberspace so that everyone can benefit from the opportunities in a digitally connected world.

Lee Hsien Loong
October 2021

Contents



Overview of the

SINGAPORE CYBERSECURITY STRATEGY 2021

A secure cyberspace underpins our national security, powers a digital economy, and protects our digital way of life.

Singapore launched our first Singapore Cybersecurity Strategy in 2016 (‘Strategy 2016’), which helped lay the foundations of our cybersecurity efforts today. As our strategic and technological environment has changed significantly over the past five years, we have reviewed and refreshed our cybersecurity strategy to address new and emerging cyber-threats.

With a robust cybersecurity workforce and a vibrant cybersecurity ecosystem as key enablers, the Singapore Cybersecurity Strategy 2021 (‘Strategy 2021’) lays out our plans to strengthen the security and resilience of our digital infrastructure and enable a safer cyberspace to support our digital way of life. It also articulates how Singapore could play an outsized role in the digital domain despite being a small country, to support an open, secure, stable, accessible, peaceful, and interoperable cyberspace.

Build Resilient Infrastructure

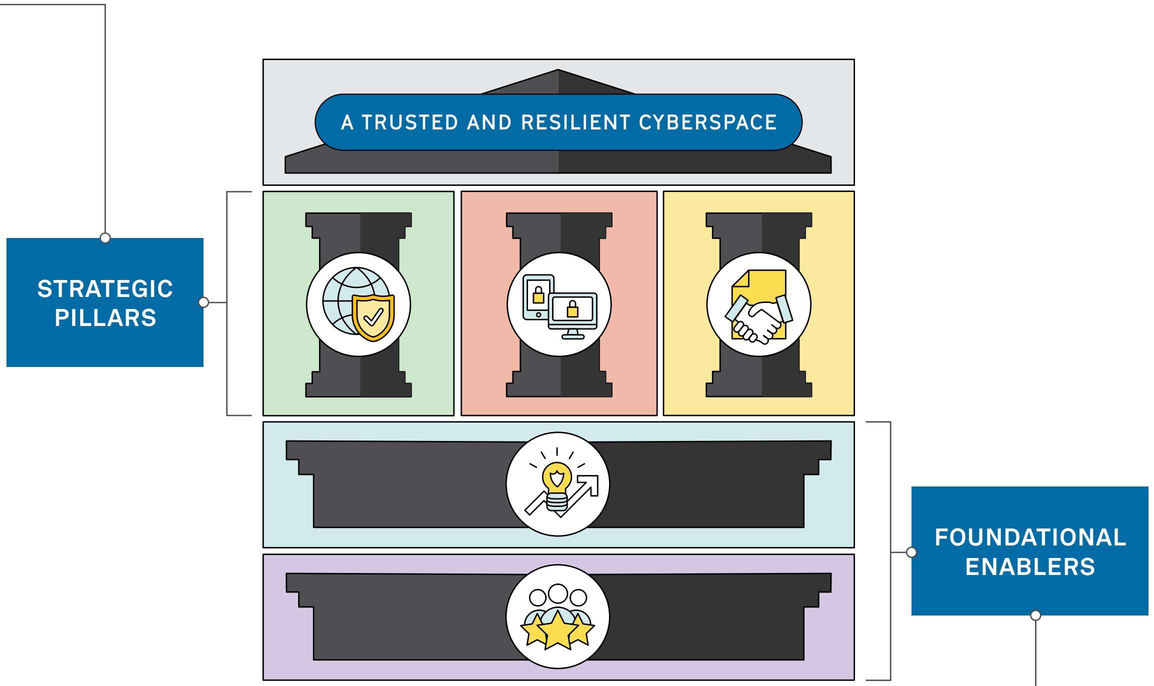
- Enable a coordinated approach to national cybersecurity with CIIs at its core
- Ensure government systems are secure and resilient
- Safeguard important entities and systems beyond CIIs

Enable a Safer Cyberspace

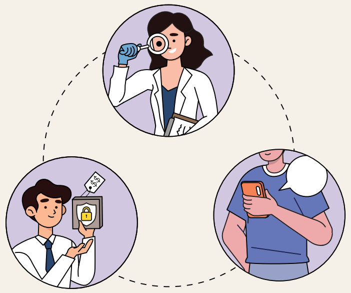
- Secure digital infrastructure, devices, and applications that power our digital economy
- Safeguard our cyberspace activities
- Empower our cyber-savvy population for a healthy digital way of life

Enhance International Cyber Cooperation

- Advance the development and implementation of voluntary, non-binding norms, which sit alongside international law
- Strengthen the global cybersecurity posture through capacity-building initiatives and the development of technical and interoperable cybersecurity standards
- Contribute to international efforts to combat cross-border cyber threats



Develop a Vibrant Cybersecurity Ecosystem



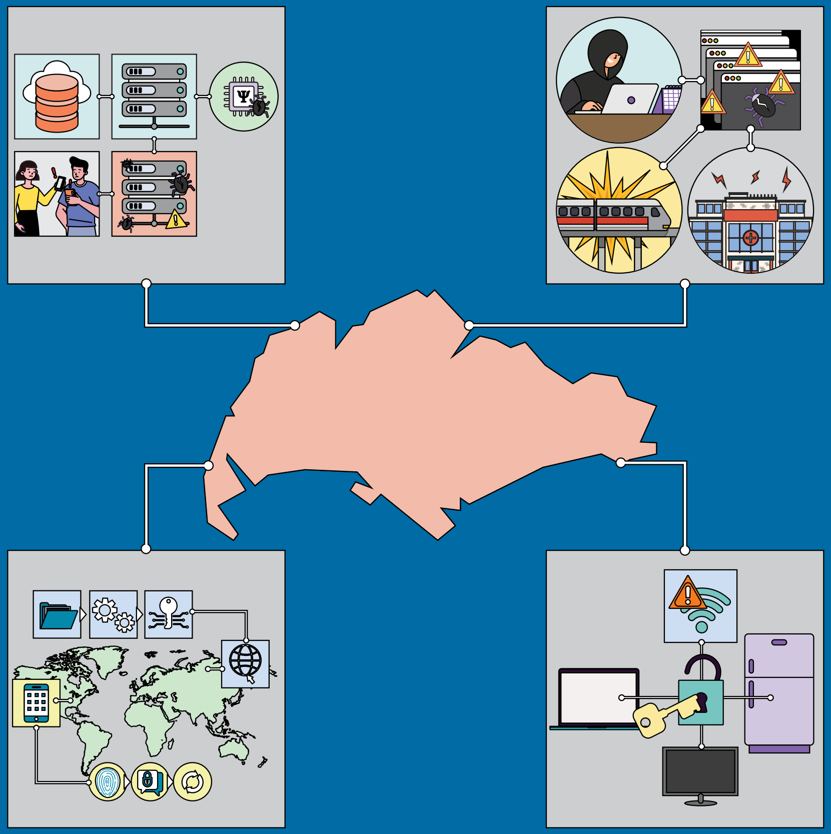
- Develop advanced capabilities for economic growth and national security
- Innovate to build world-class products and services
- Grow our cybersecurity market

Grow a Robust Cyber Talent Pipeline

- Support youths, women, and mid-career professionals to pursue a cybersecurity career
- Create an upskilling culture for a globally competitive workforce
- Foster a dynamic sector with strong professional communities

INTRODUCTION

SINGAPORE'S CYBER OPERATING LANDSCAPE



As Singapore harnesses digital technology to improve lives and livelihoods for all, cybersecurity has become a necessity and a key enabler for our digital economy and digital way of life.

Singapore takes cyber threats seriously. Our cybersecurity journey started with the first Infocomm Security Masterplan in 2005 and the formation of the Singapore Infocomm Technology Security Authority (SITSA) in 2009. In 2015, the Cyber Security Agency of Singapore (CSA) was set up as the central agency to oversee and coordinate all aspects of cybersecurity for the nation.

CSA published the first Singapore Cybersecurity Strategy in 2016, which had sought to:

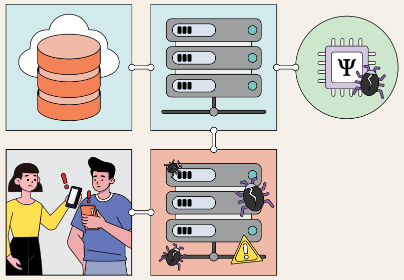
(i) Build a resilient infrastructure;
(ii) Create a safer cyberspace;
(iii) Develop a vibrant cybersecurity ecosystem; and
(iv) Strengthen international partnerships.

GO.gov.sg
https://go.gov.sg/xsp6w5

Scan here to learn more about Singapore's cybersecurity journey since 2016!

Key Shifts in our Cyber Operating Environment

The digital domain is one that is rapidly evolving. In the past five years, Singapore has observed four key shifts in our cyber operating environment:

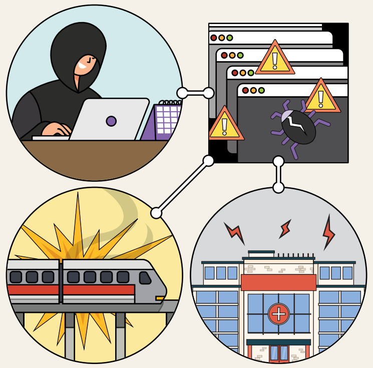


Disruptive Technologies

Looking ahead, there are several emerging technologies that may disrupt current approaches towards cybersecurity.

For example, edge computing, enabled by 5G, cloud computing, and ubiquitous access to digital devices, will fundamentally change our network environment. This requires a mindset shift, as we move away from perimeter defence towards a zero-trust cybersecurity model. Quantum technologies will also disrupt the cryptographic methods underpinning cybersecurity today.

On the flip side, technologies such as artificial intelligence and quantum computing also present us with new ways to secure our digital assets.

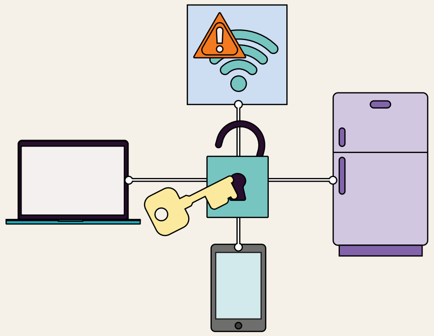


Growing Cyber-Physical Risks

We are entering an age where the digital and physical realms converge. Cyber disruptions can spill over to the physical domain with real-world consequences. In 2021 alone, we have seen the disruption of hospitals, oil pipelines, and manufacturing facilities in various countries because of cyberattacks.

Growing cyber-physical risks are not limited to the industry; these risks are also creeping into our everyday lives with the proliferation of smart devices and internet-enabled products in our homes.

We must therefore ensure our CIIs and other important systems are well protected and resilient. Existing policy and legislative frameworks must also be fit-for-purpose to address these risks.

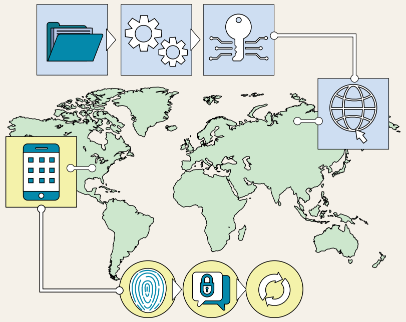


Ubiquitous Digital Connectivity

The COVID-19 pandemic has accelerated digitalisation; businesses and individuals are increasingly dependent on the smooth running of digital infrastructure and services. This has vastly expanded the attack surface for Singapore and Singaporeans, exposing more vulnerabilities to be exploited.

Cyber threat actors take advantage of this to launch cyberattacks. Cyberattacks are not only growing in volume; they are also growing in sophistication.

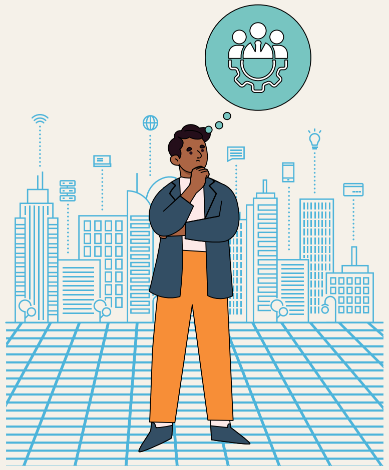
We will work with businesses and individuals so that they are equipped to mitigate and manage cybersecurity risks, so that they can digitalise safely and securely.



Increased Geopolitical Tensions in Cyberspace

Digital technologies are increasingly perceived as a key determinant in the distribution of power in the international system. The digital domain has thus become a new arena for geopolitical contestation. States are in a race to develop first-mover advantages over key digital technologies. Technical standards-setting bodies are increasingly receiving political attention.

Singapore must remain steadfast in our commitment to an open, secure, stable, accessible, peaceful, and interoperable cyberspace and actively work towards this vision, in order to navigate these geopolitical tensions.



How are we adapting to a changing cyber landscape?

Compared to Strategy 2016, Strategy 2021 takes a more proactive stance to address threats, broadens our scope of protection, and seeks to develop deeper partnerships with industry and other organisations to adapt to the changes in our cyber operating environment. Strategy 2021 also places greater emphasis on workforce and ecosystem development as key enablers of our cybersecurity.

STRATEGIC PILLARS

	Build Resillient Infrastructure	Enable a Safer Cyberspace	Enhance International Cyber Cooperation
OBJECTIVES	**Strengthen the security and resilience of our digital infrastructure**	**Create a cleaner and healthier digital environment**	**Foster an open, secure, stable, accessible, peaceful, and interoperable cyberspace**
SINGAPORE’S APPROACH	Regulation will continue to be a key lever. In Strategy 2021, we will explore expanding the Government’s regulatory remit under the Cybersecurity Act to include entities and systems beyond CIIs. However, a purely regulatory approach could engender a compliance mindset, which is not desirable in a fast-evolving environment. Enterprises and organisations should instead adopt a risk management mindset. Strategy 2021 will therefore also seek to nudge enterprises and organisations to invest in cybersecurity to thrive in a digital world.	The Government will take the lead to secure the digital infrastructure that powers our digital economy, and support the development of a healthy digital environment. Recognising that cybersecurity can seem daunting to many, the Government will also seek to make it easier for everyone to secure their devices and use secure applications. Enterprises, organisations, and individuals must play their part too. Enterprises and organisations should include cybersecurity as part of their risk management framework and strengthen their cybersecurity posture. Individuals should practise good cyber hygiene and stay vigilant against cyber threats.	Singapore will advance the development and implementation of voluntary, non-binding norms, which sit alongside international law. We will also advocate the development and adoption of technical and interoperable standards. Eventually, this will allow us to work towards a rules-based multilateral order with agreed principles for responsible State behaviour in cyberspace. We will also step up operational cooperation with our international partners to combat cross-border cyber threats. Singapore will also support capacity-building programmes to help raise the global and regional levels of cybersecurity.

FOUNDATIONAL ENABLERS

	OBJECTIVES	SINGAPORE’S APPROACH
Develop a Vibrant Cybersecurity Ecosystem	**Build a cybersecurity ecosystem underpinned by research and innovation for our security and economic needs**	To develop a vibrant cybersecurity ecosystem, the Government will galvanise the cybersecurity industry and academia to develop advanced capabilities, build world-class products and services, and grow our cybersecurity market. The Government will invest in cybersecurity research and innovation. We will also establish entrepreneurship programmes, which stakeholders can leverage to develop Made-in-Singapore solutions.
Grow a Robust Cyber Talent Pipeline	**Develop and sustain a strong cybersecurity workforce to meet our security and economic needs**	The Government will work closely with our schools to educate students in cybersecurity and nurture budding cybersecurity enthusiasts. The Government will also partner the industry and Institutes of Higher Learning (IHLs) to develop skills and competency frameworks toward structured career paths for cybersecurity professionals. In line with the national SkillsFuture movement, the Government will also encourage individuals interested in cybersecurity to further their skills through programmes offered by industry and training institutes.

What is my role?

Cybersecurity is a team sport, and everyone has a part to play. The Government will take the lead in rolling out initiatives to keep Singapore's cyberspace safe. However, this Strategy is not just a government blueprint; it is a call to action for all stakeholders to leverage resources and opportunities outlined in this Strategy to play their part and contribute to the nation's cybersecurity. The Government will play the role of team captain, guiding and empowering enterprises, organisations, and individuals to collectively work towards a safe and secure cyberspace.

I am...

A CII owner

A software or hardware vendor

A leader of an enterprise or organisation

A cybersecurity professional or researcher

A student

An individual who uses digital technology for work or play

I can...

Strengthen the security of CIIs by:

- Adopting a risk-based approach towards cybersecurity
- Incorporating cybersecurity in my enterprise's risk management framework
- Leveraging the CII Supply Chain Programme to manage vendor cybersecurity risks
- Using the Operational Technology (OT) Cybersecurity Competency Framework as a tool to establish processes, structures, or jobs to manage OT cybersecurity within my organisation

Contribute to a healthier digital environment by:

- Equipping my employees with cybersecurity skills and knowledge to build secure-by-design software and hardware products
- Applying to get my products certified under the Cybersecurity Labelling Scheme

Strengthen my organisation's cybersecurity posture by:

- Adopting a risk-based approach towards cybersecurity
- Incorporating cybersecurity in my organisation's risk management framework
- Applying for the SG Cyber Safe Trustmark for my organisation
- Using the resources and toolkits developed by CSA to raise cybersecurity awareness throughout my organisation

Contribute to our cybersecurity ecosystem by:

- Leveraging the National Cybersecurity R&D Programme to develop advanced cybersecurity capabilities
- Leveraging initiatives such as the Cybersecurity Call for Innovation to create new innovative cybersecurity solutions
- Working with local industry associations on community initiatives

Learn more about cybersecurity by:

- Participating in SG Cyber Youth programmes, such as the Youth Cyber Exploration Programme or the Cybersecurity Career Mentoring Programme
- Participating in cyber sparring and training under the SG Cyber Olympians programme

Take responsibility for my own cybersecurity by:

- Practising good cyber hygiene
- Adopting the tips in the SG Cyber Safe campaigns
- Using the appropriate cybersecurity solutions to protect my devices

CHAPTER 1

BUILD RESILIENT INFRASTRUCTURE

GOAL

Strengthen the security and resilience of our digital infrastructure

We rely on Critical Information Infrastructures (CIIs) for the provision of essential services, such as telecommunications, energy, healthcare, and banking.

With increasing digitalisation, CIIs that were previously isolated from the Internet are now increasingly linked to other digital systems, exposing them to cyber vulnerabilities and threats. At the same time, threat actors are becoming more sophisticated and are honing their craft to exploit any vulnerability they can find to disrupt our digital way of life.

The Government is committed to the security and resilience of our CIIs, even as we push for more digitalisation. Beyond CIIs, the Government will also seek to raise the cybersecurity posture of other digital systems and infrastructure that could impact Singaporeans' lives and livelihoods.

WHAT'S NEW?

In Strategy 2016, the Government focused on strengthening the cyber resilience of our CIIs. The Cybersecurity Act was passed in 2018 and serves as the legislative framework to safeguard our CIIs.

While we continue to strengthen these areas, Strategy 2021 also seeks to:

▶ Leverage synergies across the nation

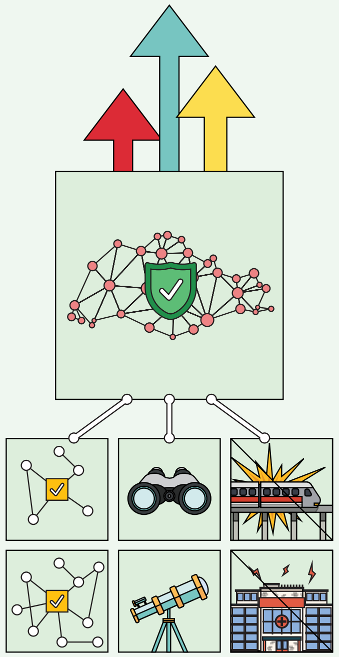
This includes strengthening our technical capabilities and enhancing coordination across the Government in order to act with greater effectiveness, speed, and agility.

▶ Broaden our scope of protection beyond CIIs

We want to strengthen the cybersecurity posture of other key entities whose compromise or disruption have significant knock-on effects to the wider economy and society.

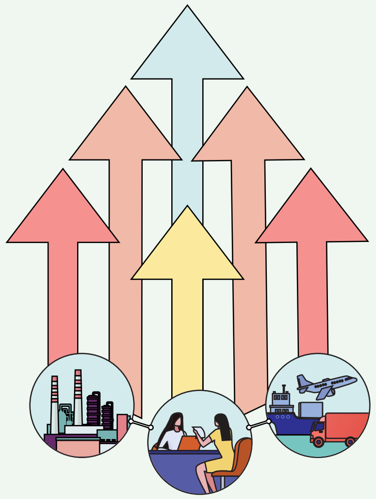
▶ Address growing cyber-physical risks

As the physical and digital worlds continue to converge, we want to ensure our policy and legislative frameworks remain fit-for-purpose to manage cyber-physical risks.



The Government will work closely with CII owners, the cybersecurity industry and key digital infrastructure owners to **enable a coordinated approach to national cybersecurity**. We will also **ensure that government systems providing key services for our citizens are secure and resilient**. The Government will also look beyond CIIs and work towards **safeguarding other entities and systems** that provide important services that support our digital economy and way of life.

Enable a coordinated approach to national cybersecurity with CIIs at its core



To ensure our essential services are well-protected from cybersecurity threats, we will evolve our policy approach to defend against sophisticated threat actors. We must also continue to strengthen capabilities to protect, detect, respond, and recover from malicious cyber activities. We will also ensure that cyber-physical risks are well managed.

Evolve our policy approach to defend against sophisticated threat actors

The Government will implement a layered and coordinated approach to national cyber defence. CII owners will be encouraged to adopt a zero-trust cybersecurity posture for critical systems. For other services and infrastructure whose disruption could have significant knock-on effects on the nation, a risk-based approach will be adopted to strengthen the cybersecurity of these systems. For example, CSA is developing a CII Supply Chain Programme to provide recommendations for all stakeholders to manage cybersecurity risks in the supply chain. In addition, we also seek to change mindsets, such that cybersecurity will be viewed as an enterprise risk management issue, as opposed to a compliance issue.

Strengthen capabilities to protect, detect, respond, and recover from malicious cyber activities

Cybersecurity is enabled by strong capabilities. The Government will strengthen our technical capabilities to detect and analyse malicious cyber activities to better defend against such threats. This includes the development of a Cyber Fusion Platform that will allow the Government to conduct investigation with enhanced speed and efficiency. To strengthen our response and recovery, the Government will also implement initiatives such as the new National Cyber Security Command Centre. We will also work with CII owners and other organisations to address the various people, process, and technology challenges in cybersecurity.

Ensure policy and legislative frameworks remain fit-for-purpose to address growing cyber-physical risks

The effects of cyberattacks are no longer contained in the digital domain. They are spilling into the physical realm, as evidenced by ransomware attacks on the Colonial Pipeline Company in the US and healthcare services in Ireland and New Zealand. Our policy and legislative frameworks must evolve and adapt to mitigate cyber-physical risks. This includes reviewing the Cybersecurity Act, as well as introducing policy initiatives such as the OT Cybersecurity Masterplan and OT Cybersecurity Competency Framework.

Critical Information Infrastructures in Singapore

CIIs are digital systems that support the delivery of essential services. Today, CIIs have been identified from 11 critical sectors — Aviation, Banking & Finance, Energy, Government, Healthcare, Infocomm, Land Transport, Maritime, Media, Security & Emergency Services, and Water.

To ensure that our essential services are not disrupted by cyber threats, the Government has put in place a three-tier framework to strengthen the cyber resilience of CIIs.

- CSA, as the independent national authority on cybersecurity, monitors and regulates the CII sectors. At the same time, CSA actively supports sector leads and CII owners to improve their situational awareness and build up their capabilities.
- Each CII sector has a sector lead, who works closely with CSA. They are the natural regulators of the CII owners and have a good grasp of the unique operating and business environment — and risks — of their respective sectors. They are best placed to provide guidance on the appropriate balance point of cybersecurity, usability, and cost.
- At the organisational level, CII owners are responsible for managing their cybersecurity risks and are the first line defenders and responders.

Ensure government systems are secure and resilient

To enable public service digitalisation, the Government will ensure that all government systems — including both CIIs and non-CII systems — are resilient, protected, and trusted by its users. Today, all government systems comply with tailored cybersecurity policies that are reviewed periodically. We will also modernise the cybersecurity architecture of government systems to stay ahead of technological developments. Cybersecurity is not only about technology, but also about people and organisational processes. We will therefore also raise the level of cybersecurity competency across Government. We hope that the Government's risk-based approach towards cybersecurity can serve as a guide for other organisations and enterprises looking to strengthen their cybersecurity posture.

Review cyber policies and enforce a tiered set of requirements in Government

Instructional Manual 8 (IM8) is the management tool used in Government to safeguard government ICT & Smart Systems (ICT&SS) assets. The IM8 Policy on Security establishes tailored security hygiene practices for government systems, based on a system's classification and criticality. The Smart Nation and Digital Government Group (SNDGG) supports the implementation of IM8 security controls by providing consultancy services and deploying Chief Information Security Officers (CISOs) across Government. The Government also conducts regular penetration testing on government systems as part of the IM8 audit, identifying vulnerabilities to be addressed before potential exploitation.

Modernise the cybersecurity architecture in Government

The Government is implementing the Government Trust-based Architecture (GTbA) that translates zero-trust principles to the Government context, thereby strengthening the security of applications and systems.

To complement the GTbA, the Government will operationalise the Government Cybersecurity Operations Centre (GCSOC) that can provide real-time monitoring, increase Government's situational awareness, and allow a more rapid and accurate incident response.

Raise the level of cybersecurity competency across Government

As we become more reliant on digital systems, the Government must ensure that public officers are well equipped with the skills and knowledge to keep themselves cyber safe. The Government will also develop a Cybersecurity Functional Competency Framework to provide clear development milestones for government cybersecurity specialists. In addition, SNDGG has launched the GovTech Digital Academy that will provide customised cybersecurity training programmes for ICT&SS professionals in Government.

The Government Bug Bounty Programme and Vulnerability Disclosure Programme

The Government Bug Bounty Programme (GBBP) is a programme that invites established cybersecurity researchers to conduct targeted assessments on critical government systems with a bounty reward for critical vulnerabilities discovered. On the other hand, the Vulnerability Disclosure Programme (VDP) is a crowdsourcing platform for the public to identify and report vulnerabilities in government internet-facing mobile and web-based applications. Through this platform, SNDGG encourages responsible reporting of any suspected vulnerability while strengthening the sense of collective ownership over the cybersecurity of government systems.

Building on the success of the GBBP and VDP, SNDGG launched the new Vulnerability Rewards Program (VRP) in 2021. Together, the three crowdsourced vulnerability discovery programmes supplement Govtech's suite of initiatives to safeguard Government systems.

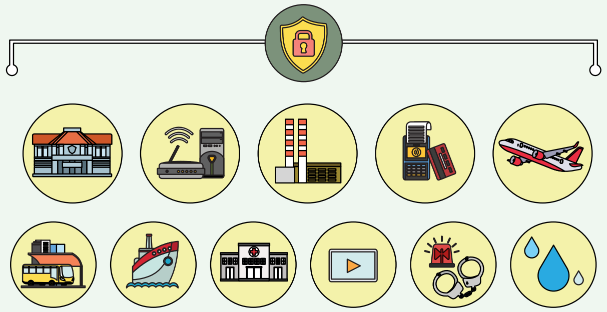
Vulnerability Rewards Programme (VRP)

https://go.gov.sg/nyfzgz

Vulnerability Disclosure Programme (VDP)

https://go.gov.sg/grjvck

Safeguard important entities and systems beyond CIIs



With increasing reliance on digital infrastructure and services, the Government must look beyond CIIs to support the cybersecurity of other entities, especially if their disruption will have significant knock-on effects to the rest of Singapore. We will also address the risks of new digital operating models, so that Singaporeans can confidently unlock the benefits of new technologies with peace of mind.

Raise cybersecurity posture of important systems and entities beyond CIIs

While cyber regulations around the world are largely focused on preventing the disruption of essential services, there are some systems and entities that do not deliver essential services but can nevertheless have a significant impact on Singapore if disrupted or compromised. In this regard, we must likewise raise their cybersecurity posture to protect that our digital economy and way of life. The Government will study the wider digital landscape and ensure that these significant systems and entities are adequately protected against malicious cyber threats.

Address cybersecurity risks arising from new digital operating models

Digital technologies will always evolve, and we must be ready to adapt to the new operating models that emerge as a result. For example, cloud services are increasingly important for the provision of digital services supporting key business functions and operations. The Government will study the public policy implications of emerging digital operating models and seek to address the risks as appropriate.

CHAPTER 2

ENABLE A SAFER CYBERSPACE

GOAL

Create a cleaner and healthier digital environment

Digitalisation has changed the way we live, work, and play. Cybersecurity is a key enabler for Singaporeans to digitalise confidently and safely.

Our goal is to create a healthy digital environment. Just as how good physical hygiene goes a long way to keep us healthy, a cleaner digital environment and good cyber hygiene practices will help keep us safe in the digital world. In 2020, the Government launched the Safer Cyberspace Masterplan, which articulated our approach to creating a clean and healthy digital environment. The Masterplan remains relevant to Strategy 2021.

Scan to read the Safer Cyberspace Masterplan

WHAT'S NEW?

Strategy 2016 had sought to raise awareness and encourage adoption of good cyber hygiene. Despite the high level of awareness of the need for cybersecurity, adoption of cyber safe practices amongst enterprises and individuals remains low.

As articulated in the Safer Cyberspace Masterplan, the Government seeks to raise the general level of cybersecurity in Singapore by:

▶ Offering cybersecurity to the masses

The Government will protect our national Internet infrastructure such that enterprises and individuals in Singapore are protected from most online threats ever reaching them.

▶ Simplifying cybersecurity for end-users

The Government will make the adoption of cybersecurity solutions easy and convenient. The Government will also work with the industry to develop innovative cybersecurity solutions for end-users to plug and play.

Everyone has a role to play in enabling a safer cyberspace. The Government will champion the effort but enterprises, individuals and the wider community must also come on board. Together, we can work towards **securing the digital infrastructure, devices, and applications** that powers our digital economy; **safeguarding our cyberspace activities**; and **empowering our cyber-savvy population** for a healthy digital way of life.

Secure digital infrastructure, devices, and applications that power our digital economy

Apart from securing key digital infrastructure as mentioned in Chapter 1, we can protect Singapore and Singaporeans by minimising vulnerabilities in our Internet architecture. However, not all threats can be detected or prevented at the national level. We will also empower individuals to secure their devices and work with enterprises to strengthen the security of their applications.

Protect Singapore's Internet infrastructure

The Government can provide an additional layer of protection to all Singaporeans by securing our national Internet infrastructure. For example, the Government is working with the Internet Service Providers to implement the Domain Name System Security Extension (DNSSEC) protocol across local Internet domains. This augments the security of the Internet, thereby preventing cyber threats from ever reaching end-users.

Secure user devices and endpoints

Vulnerabilities are commonly found in devices and endpoints. Due to the competitive ICT market, many manufacturers often prioritise features, usability, or cost over the security of the device. The Government is encouraging businesses to invest in the security of their products. For example, we launched the Cybersecurity Labelling Scheme in 2020, which allows consumers to easily assess the level of security of a smart device.

Safeguard enterprise applications

Applications are the interface between the user and cyberspace. Malicious actors can leverage vulnerabilities in applications to access users' sensitive information. To incentivise Software-as-a-Service (SaaS) platforms to develop more secure applications, we will be looking into initiatives such as labelling schemes for SaaS products. We will also strengthen our partnership with the private sector, which manages most digital applications, to ensure that their products are secure.

Safeguard our cyberspace activities

A cyber breach is a matter of when, not if. We must therefore be able to quickly detect and remediate such breaches. As mentioned in Chapter 1, the Government will strengthen capabilities to protect, detect, respond, and recover from malicious cyber activities. We will also enable enterprises to protect themselves against cyber threats and support them to put in place baseline standards of data protection.

Enable enterprises to protect themselves against cyber threats

The Government will support enterprises by making cybersecurity resources available — from free self-help tools to cost-effective solutions provided in partnership with the cybersecurity industry. For example, as we become more reliant on mobile devices for work and leisure, cyber criminals will also increasingly target these devices. The Government will work with the industry to develop a mobile endpoint solution for citizens to secure their mobile phone from threats, while upholding personal privacy.

Support organisations to put in place baseline standard of data protection

The Government will enhance our offering of tools and self-help platforms for enterprises to strengthen data protection. The Government will also work with the industry to provide data protection services such as Data Protection-as-a-Service for Small and Medium Enterprises (SMEs). This will provide SMEs with limited resources the support they need to meet data protection requirements.

Using data and artificial intelligence responsibly

The Government is committed to supporting our enterprises to use data responsibly to derive business value.

The Better Data Driven Business (BDDB) programme provides free tools and guidance to help enterprises better safeguard their customers' personal data while using data effectively to remain competitive. The BDDB aims to support SMEs that are new to data analysis, as well as SMEs looking to leverage data for more complex use cases. The BDDB will also be a one-stop shop for guidance on data protection practices, as well as professional data protection services for enterprises.

The Infocomm Media Development Authority (IMDA) and the Personal Data Protection Commission (PDPC) have also been guiding industry in developing and deploying trustworthy artificial intelligence (AI) systems. Past initiatives include the Model AI Governance Framework, the Implementation and Self-Assessment Guide for Organisations (ISAGO), and two volumes of Compendium of Use Cases. IMDA and PDPC have also developed a draft AI governance testing framework and are working with like-minded partners to make this a Minimum Viable Product (MVP). It is envisioned that this MVP will support industry in meeting the specifications of key AI governance frameworks, such as those from European Union, the OECD, and Singapore.

Better Data Driven Business

https://go.gov.sg/ymjqfl

Model AI Governance Testing Framework

https://go.gov.sg/0chi0d

Empower our cyber-savvy population for a healthy digital way of life

A lack of awareness or lax attitudes towards cybersecurity among end-users can be the Achilles' heel of even the most secure systems. To empower our population to take charge of their online safety, we will raise awareness and change attitudes on cybersecurity and promote adoption of good cyber practices.

Raise awareness and change attitudes on cybersecurity

The Government will roll out national cybersecurity awareness campaigns to drive greater awareness and encourage adoption of good cyber hygiene practices. The Government will also organise targeted outreach for specific segments of the population such as students, working adults, and seniors. We will do this in collaboration with the private sector to expand our reach.

Promote adoption of good cyber practices

In addition to raising awareness, the Government will support and encourage individuals and enterprises to protect themselves online. For example, CSA's Go Safe Online portal provides actionable advice and tips for the public and enterprises. CSA will also launch a voluntary SG Cyber Safe Trustmark and cyber hygiene mark for enterprises. The marks will allow enterprises to have a clear picture of their cybersecurity level, and reassure their customers that their systems are secure.

Working together to strengthen our collective cyber resilience

The Government undertakes regular campaigns to raise awareness on cybersecurity and combat cybercrime. For example, CSA launched the "Better Cyber Safe than Sorry" campaign in June 2021 to promote and encourage the adoption of good cyber hygiene practices. The Singapore Police Force (SPF) also organises a nationwide anti-scam public education campaign annually.

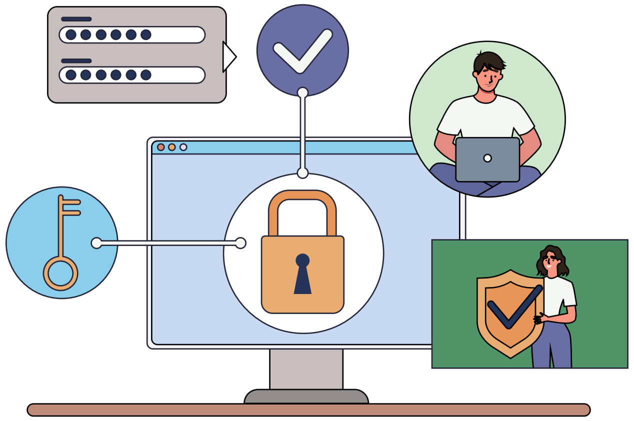
Better cyber safe than sorry
You wouldn't use a weak door lock to keep your home safe.
Use strong passwords and enable 2FA to secure your accounts.
You wouldn't share your personal information with strangers.
Be vigilant and learn to spot signs of phishing.
You wouldn't leave yourself unprotected against viruses.
Use anti-virus software to prevent malware infections.
You wouldn't rely on a leaky umbrella to keep you dry.
Patch your software promptly to protect your devices.

CSA's "Better Cyber Safe than Sorry" Campaign

The NPCC Cybercrime Prevention Programme (photo taken before COVID-19)

The Government also raises awareness amongst the more vulnerable groups of the population. The SG Cyber Safe Seniors Programme that was launched by CSA, SPF, and IMDA in 2021 aims to reach 50,000 seniors over two years. The programme will cover topics such as cyber threats, online scams, and cyber tips in four languages through webinars, publications and face-to-face engagements. The Government also reaches out to students through programmes such as the National Police Cadet Corps (NPCC) Cybercrime Prevention Programme and the SG Cyber Safe Students Programme.

Private sector stakeholders play an important role. To tackle cybercrime, the SPF established the Alliance of Public Private Cybercrime Stakeholders (APPACT) in 2017. APPACT has since grown to a 59-member strong alliance across nine industries, including banks, e-commerce, and social media platforms. The SPF conducts regular outreach and discussions with APPACT partners to chart new ways to tackle cybercrime. With APPACT members' efforts and vigilance in preventing and detecting cybercrime, there have been numerous success stories arising from the close partnerships forged via this public-private industry platform.



SG Cyber Safe Trustmark and cyber hygiene mark

Cybersecurity can be a competitive advantage. Businesses are digitalising faster than ever; cybersecurity will be key to securing the trust of consumers, especially given the increasing frequency of cyber breaches.

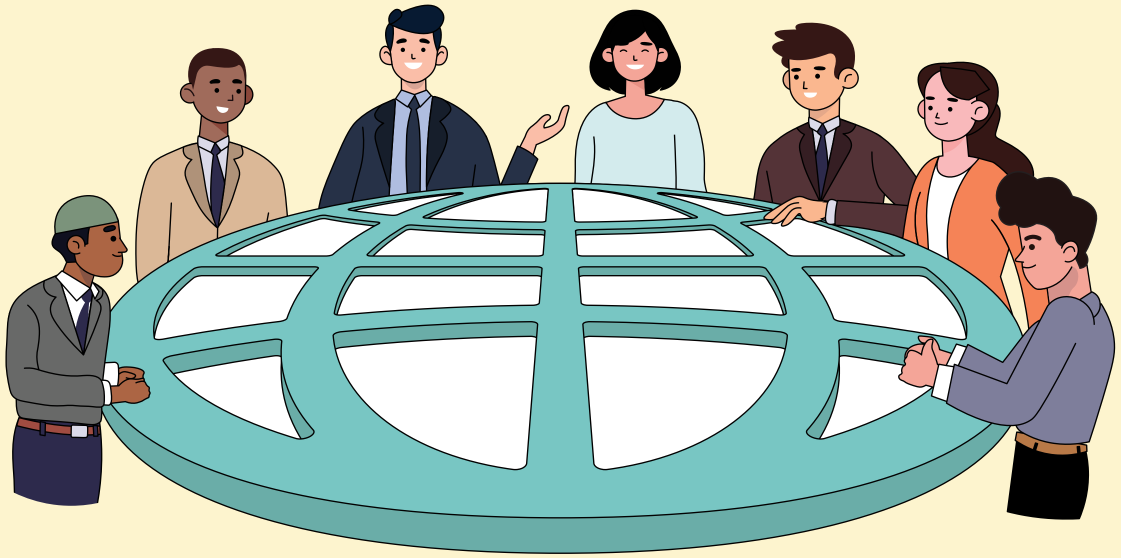
CSA is introducing a voluntary SG Cyber Safe Trustmark, which will serve as a mark of distinction to recognise companies with good cybersecurity measures. This will allow customers to make an informed choice on the companies to engage, based on their cybersecurity posture.

For smaller enterprises that may not have dedicated IT or cybersecurity expertise, CSA is developing a separate cyber hygiene mark. This cyber hygiene mark is designed to be practical and implementable, focusing on basic cyber hygiene, so that businesses are better protected from common cyberattacks.

Both the Trustmark and cyber hygiene mark are being developed in consultation with industry practitioners.

CHAPTER 3

ENHANCE INTERNATIONAL CYBER COOPERATION



GOAL

Foster an open, secure, stable, accessible, peaceful, and interoperable cyberspace

Cyber threats are international and cross-border.

We have seen significant cyberattacks spill over country lines, from the SolarWinds breach, to the Kaseya Virtual System Administrator (VSA) attack.

A resilient infrastructure and a safer cyberspace support our domestic resilience against cyber threats. However, we also need to engage and collaborate with our international partners to work towards the longer-term objective of a rules-based multilateral order in cyberspace, and develop mechanisms and policies to raise the global baseline level of cybersecurity.

WHAT'S NEW?

The implementation of Strategy 2016 saw Singapore step up our participation in international cyber policy discussions. We have strengthened collaboration with our Association of Southeast Asian Nations (ASEAN) counterparts to improve the collective cybersecurity of the region and forged strong bilateral cybersecurity partnerships with other international partners.

As cybersecurity gains traction in global conversations, Singapore will raise our level of participation in international cyber policy discussions further by:

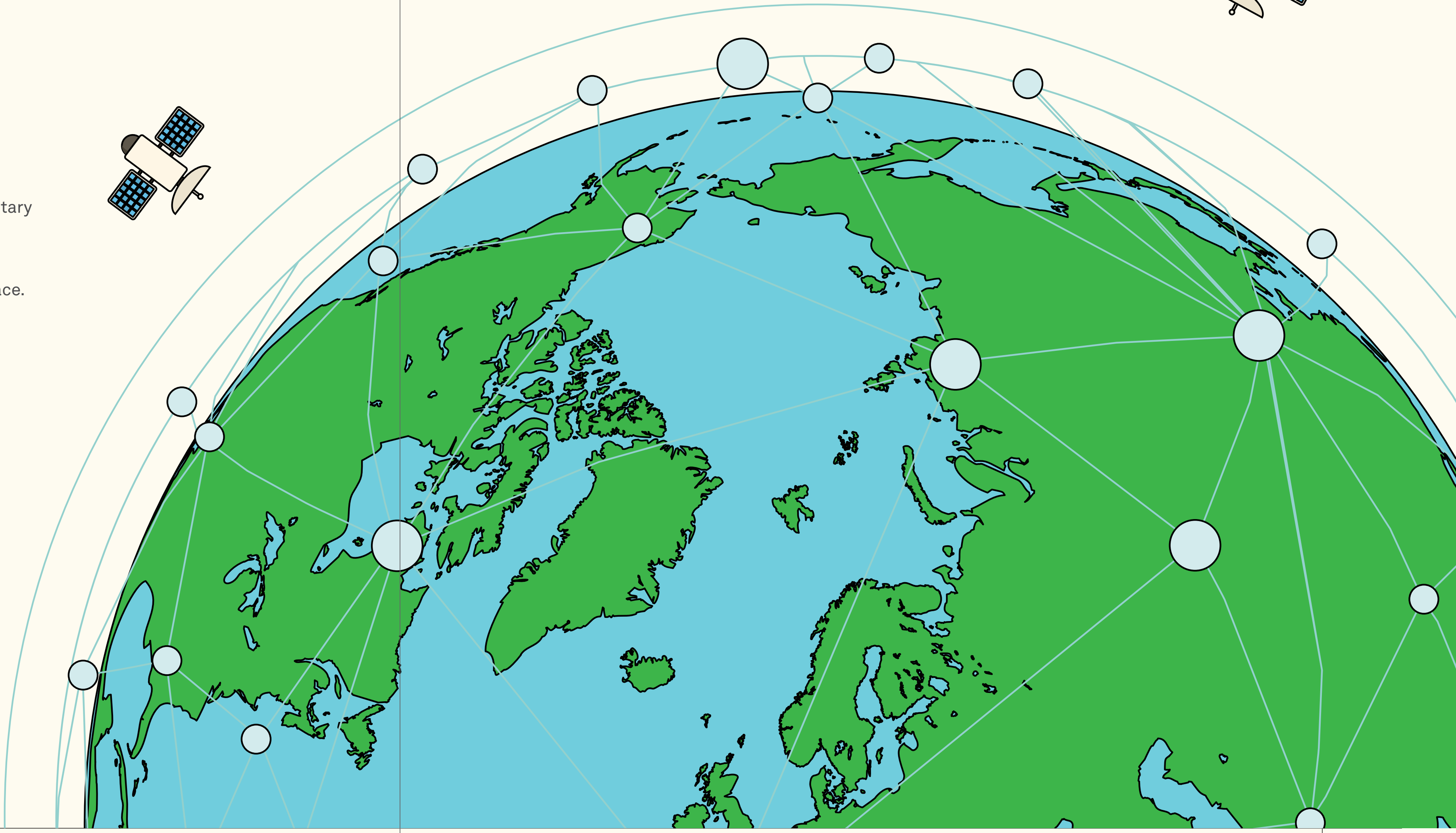
▶ Advocating a rules-based multilateral order in cyberspace and an interoperable ICT environment

As a small State, Singapore firmly supports the establishment of a rules-based multilateral order. Developing and implementing voluntary and non-binding norms are important steps toward this objective. We must help develop and abide by rules that all States agree to follow, which in turn guide responsible State behaviour in cyberspace.

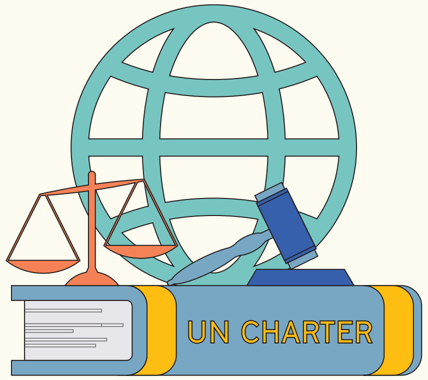
▶ Raising the global baseline level of cybersecurity

We want to support the global effort to raise the capacities of States to protect themselves against cyber threats. We also want to encourage the development and implementation of cybersecurity standards such that a minimum level of cybersecurity exists in the ICT products and services we use.

To foster an open, secure, stable, accessible, peaceful, and interoperable cyberspace, Singapore will **advance the development and implementation of cyber rules, norms, principles, and standards.** We will also **strengthen the global cybersecurity posture** and **contribute to international efforts to combat cross-border cyber threats and cybercrime**.



Advance the development and implementation of voluntary, non-binding norms, which sit alongside international law



Strategy 2021 seeks to build on the progress made by the international community. We will advance the development of cyber norms and affirm the applicability of international law in cyberspace. We will also work with partners to implement these cyber norms.

Advance international cyber norms discussions and the understanding of the application of international law in cyberspace

The United Nations (UN) is an important platform that offers all countries an opportunity to engage in and develop rules, norms, principles, and standards. Singapore has participated actively in international discussions at the UN, such as the UN Group of Governmental Experts. At these platforms, Singapore has affirmed that international law, in particular the Charter of the UN, applies to cyberspace, and underscored the centrality of States' adherence to the cyber normative and stability framework. Going forward, Singapore will actively seek to contribute and move these discussions forward. For example, Singapore will be chairing the Open-Ended Working Group on Security of and in the Use of ICTs (2021–2025).

Work with partners to implement cyber norms

In 2018, ASEAN became the first regional organisation to subscribe in-principle to the 11 voluntary, non-binding norms of responsible State behaviour in cyberspace. As part of ASEAN's next steps, Singapore is working with partners such as the UN Office of Disarmament Affairs (UNODA) and Malaysia to develop a regional action plan to implement these norms. Under the UN-Singapore Cyber Programme, we will also work with our ASEAN and global partners to develop a Norms Implementation Checklist – akin to a set of actions that countries could take to implement these norms.

Singapore International Cyber Week and the ASEAN Ministerial Conference on Cybersecurity

SICW
ASEAN MINISTERIAL CONFERENCE ON CYBERSECURITY OPENING CEREMONY
SG

The 5th ASEAN Ministerial Conference on Cybersecurity (AMCC) in 2020

Recognising the need to forge deeper public-private partnerships, Singapore has facilitated multi-stakeholder dialogues on cybersecurity through hosting the annual Singapore International Cyber Week (SICW) since 2016. SICW brings together international and regional policy makers, industry partners, and academia to discuss cross-cutting cybersecurity issues. Singapore also hosts the ASEAN Ministerial Conference on Cybersecurity (AMCC), chaired by Singapore's Minister-in-charge of Cybersecurity, on the side lines of SICW. The AMCC serves as a non-formal platform that brings together the ASEAN Secretary General and ASEAN Ministers of Telecommunications and/or Cybersecurity to discuss cybersecurity issues affecting our region and beyond.

Singapore International Cyber Week's Official Webpage

Strengthen the global cybersecurity posture through capacity-building initiatives and the development of technical and interoperable cybersecurity standards

Apart from the development and implementation of cyber norms, it is important that States work together to raise the global baseline level of cybersecurity. To this end, Singapore will support capacity-building initiatives and promote the development of technical and interoperable cybersecurity standards for products and services.

Support capacity building for a secure and stable cyberspace

In the hyper-connected cyberspace, we are only as strong as our weakest link. As global discussions on cybersecurity expand beyond traditional cybersecurity topics into emerging technologies and digital security, there is a need for capacity building to support nations in responding to the changing cyber threat landscape. Singapore will work closely with our ASEAN Dialogue Partners, industry and academic partners.

Promote the development and adoption of objective technical cybersecurity standards

Singapore recognises that standards and certifications are important tools to help raise the cybersecurity baseline of products and services in the market. Singapore is committed to the development and adoption of technical and interoperable cybersecurity standards internationally. We will build on existing efforts such as the Common Criteria, an international standard that allows for mutual recognition of secure IT products. Singapore is also working towards the mutual recognition of local schemes like CSA's Cybersecurity Labelling Scheme to improve the security of consumer IoT products globally.

ASEAN-Singapore Cybersecurity Centre of Excellence

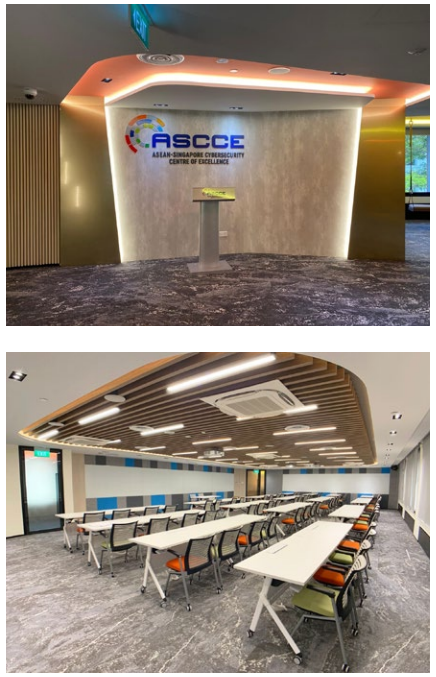
The ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) was launched in 2019 as part of the ASEAN Cyber Capacity Programme to support a coordinated build-up of cyber policy, operational, and technical capacities amongst senior ASEAN officials. The campus officially opened in October 2021.

With a funding commitment of S$30 million, the ASCCE engages top cybersecurity experts and trainers to design and deliver cybersecurity capacity-building programmes, in collaboration with ASEAN Member States (AMS), ASEAN Dialogue Partners, international partners, and the UNODA.

The ASCCE has three principal functions. First, it conducts research and provides training on cybersecurity strategy, legislation, and implementation of international cyber norms. Second, the ASCCE provides training for Computer Emergency Response Teams (CERTs), focusing on technical skills and information sharing. Third, in partnership with Temasek Polytechnic, ASCCE provides participants with hands-on practicals through virtual cyber defence training and exercises.

While the COVID-19 pandemic halted in-person capacity-building initiatives, the ASCCE has adapted our programmes for delivery on digital platforms. In 2020, the ASCCE trained over 300 AMS officials through seven virtual capacity-building programmes.

Looking ahead, the ASCCE will continue to be responsive to the region's capacity building needs, providing programming in line with the changing digital landscape to equip officials with the capacities to strengthen cybersecurity in ASEAN and beyond.



The ASCCE campus

Contribute to international efforts to combat cross-border cyber threats

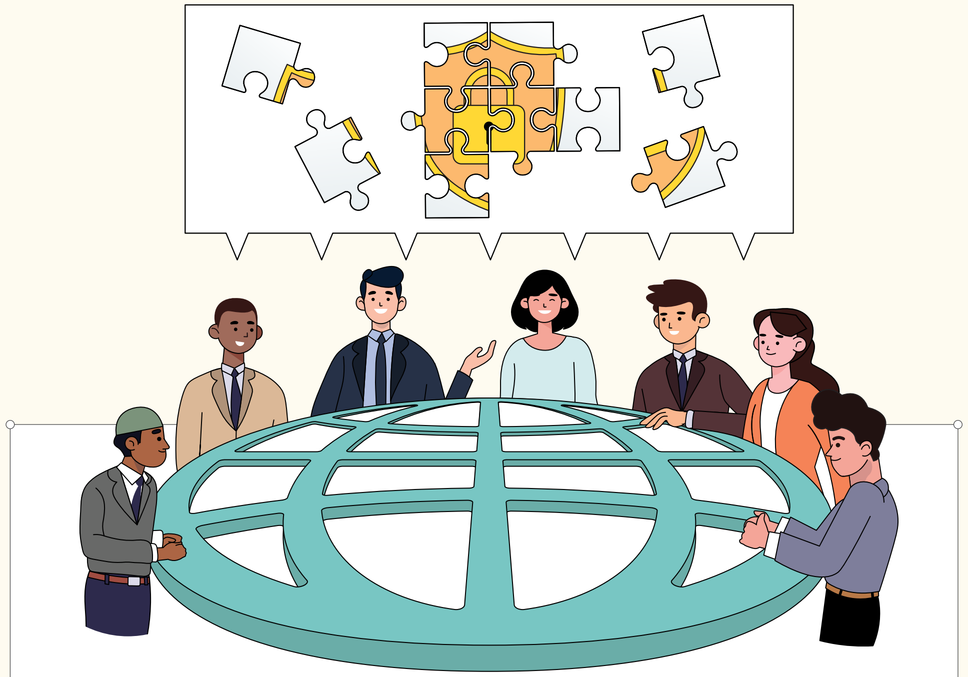
Even as we work towards a rules-based multilateral order in cyberspace and raise the global baseline level of cybersecurity, cyberattacks will inevitably happen from time to time. Examples such as the 2021 Microsoft Exchange Server breach demonstrate that cyber threats are not confined within geographical boundaries. Bilateral and multilateral operational cooperation are thus key to share timely information and respond to these incidents swiftly.

Maintain robust bilateral cybersecurity ties with key countries

Building on existing partnerships and bilateral agreements, Singapore will enhance our engagements with key international partners through regular dialogues to facilitate the sharing of operational and technical information. Beyond operational cooperation, Singapore is also looking to exchange best practices in cyber policy, ecosystem, and workforce development with our counterparts, and coordinate our capacity-building efforts to strengthen global cybersecurity.

Strengthen multilateral cooperation to tackle cross-border cyber challenges

Singapore will strengthen multilateral cooperation with our regional and international partners. Today, Singapore participates actively in various international CERT networks and work closely with CERT counterparts to investigate cyber incidents and mitigate cyber threats. We also work closely with INTERPOL as well as private sector partners to combat cross-border cybercrime. Regionally, Singapore conducts the annual ASEAN Cyber Incident Drill (ACID) and is part of the ASEAN Information Exchange Mechanism. Singapore will build on these efforts and work more closely with our partners to collectively combat cross-border cyber threats.



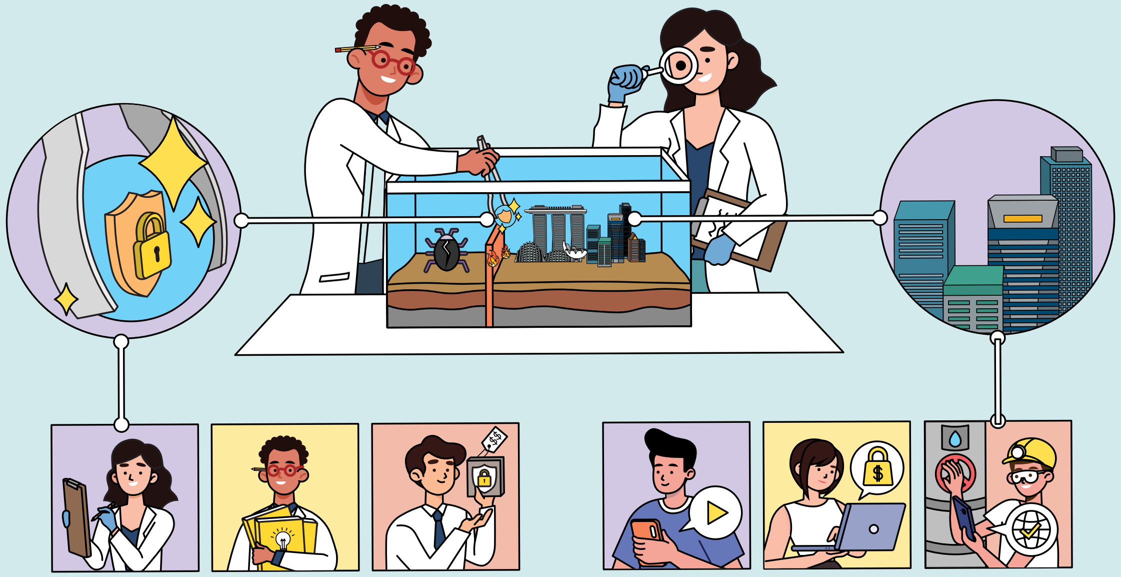
ASEAN CERT and ASEAN Information Exchange Mechanism

The ASEAN CERT will be a mechanism to tighten coordination and enhance collaboration as listed in the ASEAN Cybersecurity Cooperation Strategy 2017–2020. With Singapore as the lead, ASEAN is currently studying the implementation of the ASEAN CERT.

In addition, the first ASEAN Digital Ministers' Meeting in January 2021 approved the establishment of an ASEAN CERT Information Exchange Mechanism. This initiative will further support the ASEAN CERT-CERT cooperation to bolster the effectiveness of regional incident response capabilities. It will also facilitate future exchanges amongst all CERTs in ASEAN and coordinate CERT capacity-building programmes in the region through the ASCCE.

CHAPTER 4

DEVELOP A VIBRANT CYBERSECURITY ECOSYSTEM



GOAL

Build a cybersecurity ecosystem underpinned by research and innovation for our security and economic needs

A vibrant cybersecurity ecosystem lays the foundation for protecting Singapore from cyber threats in the longer term. It also strengthens Singapore's position as a trusted global business hub and provides economic opportunities for Singaporeans and Singapore-based companies.

For Singapore to be a global leader in cybersecurity, the Government, industry, and academia will have to work closely together. We hope to grow and nurture an ecosystem of cybersecurity companies, innovators, and researchers, who can build and develop advanced cybersecurity capabilities and best-in-class products and services of high economic value.

WHAT'S NEW?

Strategy 2016 was successful in laying the foundations for a local cybersecurity ecosystem of companies. We have catalysed the development of several Made-in-Singapore solutions and supported individuals and start-ups in establishing and scaling up their businesses.

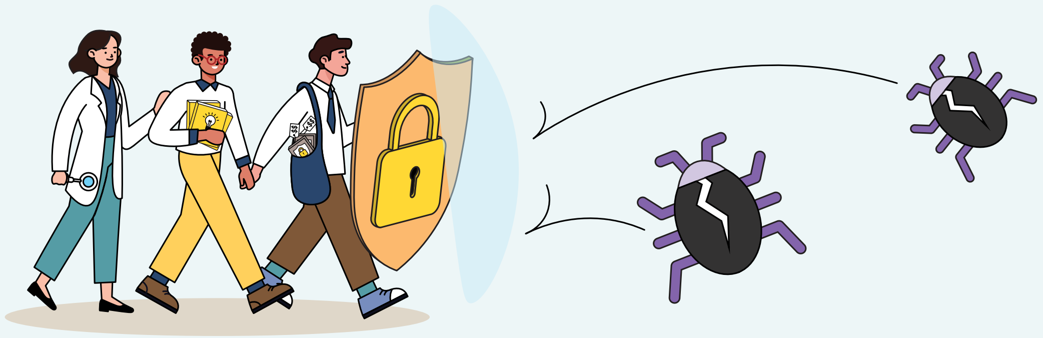
In Strategy 2021, we will take further steps to:

▶ Position Singapore as a trusted tech hub

We want to establish ourselves as an internationally recognised and trusted Testing, Inspection, and Certification (TIC) hub. Having strong security evaluation and testing capabilities will help bolster the SG Digital Economy brand.

▶ Leverage research and innovation as a competitive advantage

We want to be at the forefront of cybersecurity research and development (R&D) to keep pace with the rapidly evolving technological landscape and leverage new technologies to stay ahead of malicious cyber actors.



The cybersecurity industry and academia are key stakeholders in this national effort. The Government will work closely with them to **develop advanced capabilities**, encourage industry innovation to **build world-class products and services,** and **support the growth of the cybersecurity market.**

Develop advanced capabilities for economic growth and national security

To ensure the availability of cutting-edge capabilities amidst rapid technology change, the Government will actively facilitate the translation of research findings into commercial products, while supporting the development of our local R&D ecosystem. We will also invest in and build deep cybersecurity capabilities for our national security needs, both within Government and with industry partners.

Translate research into innovative and economically viable products

The Government will continue to work with researchers and end-users to shape the direction of cybersecurity R&D, such that research conducted can be directly applied to solve real-world challenges. We will also be working closely with industry to translate research findings into commercial products to meet our security and economic objectives. We will seek to include end-users early in the R&D process, and grow the number of collaborations between academia and the cybersecurity industry to create more pathways for research translation. The National Cybersecurity R&D Programme (NCRP) will be a key vehicle for the implementation of these policies.

Build up deep cybersecurity capabilities in Institutes of Higher Learning, the Government, and industry partners

To support our national cybersecurity needs, the Government will be investing more in the development of deep cybersecurity capabilities. The Government also recognises that such investment can benefit the local cybersecurity industry's capability development. The Government will therefore catalyse deep capability build-up in the local cybersecurity industry, especially in areas that are of strategic value to Singapore's cyber defence, by working with selected industry partners. This is augmented by ongoing efforts to attract top international companies with deep cybersecurity capabilities to set up engineering or R&D facilities in Singapore.

Innovate to build world-class products and services

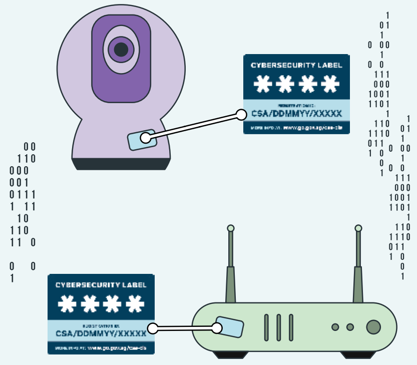
We hope to foster innovation that pushes the boundaries of cybersecurity products and services. We will achieve this by supporting industry innovation with targeted government initiatives. We will also support the growth of cyber entrepreneurs and start-ups in Singapore. Looking beyond our shores, we aspire for our enterprises to develop cybersecurity products that are recognised internationally.

Support industry innovation

Given the rapidly evolving cyber threat landscape, cybersecurity firms need to constantly innovate and invest in new solutions to stay ahead of the curve. The Government will strengthen support for industry-led innovation in cybersecurity. For example, the Cybersecurity Industry Call for Innovation encourages companies to innovate and address pressing cybersecurity challenges by matching them with key local users, such as CII owners, who may have specific operational needs. This initiative also helps provide opportunities for local companies to tap into Singapore's growing cybersecurity market and drive demand in our local cybersecurity industry.

Support growth of cyber start-ups

Apart from supporting established cybersecurity firms, it is also important to encourage budding cyber entrepreneurs and start-ups. The Innovation Cybersecurity Ecosystem at Block 71 (ICE71) is one such initiative. ICE71 programmes provide support for innovators and startups at all growth stages. This includes community outreach and entrepreneurship programmes to engage the cybersecurity ecosystem community and promote collaboration between stakeholders. We will build on our programmes to encourage entrepreneurship, including developing the next phase of ICE71.



Develop cybersecurity products that are recognised internationally

To enhance the recognition of local security products in the global marketplace, we need to ensure that these products meet the relevant international standards. Singapore has implemented the Singapore Common Criteria Scheme which evaluates and certifies IT products against the international Common Criteria standard. We have also established the Cybersecurity Labelling Scheme for consumer smart devices. We will expand these schemes and make it easier for companies to submit their products for security evaluation and testing. Building on these achievements, we seek to develop a thriving local TIC ecosystem that is internationally recognised.

National Integrated Centre for Evaluation

The National Integrated Centre for Evaluation (NICE) is a one-stop facility for security evaluation and testing of products. It will also be a platform for the local community to develop their skills in this domain.

NICE seeks to achieve the following objectives:

- To seed a community of practice for product evaluation and certification in Singapore, NICE will improve access to advanced equipment required for security evaluation at the highest assurance level.
- To support the growth of the local cybersecurity TIC industry, NICE will provide opportunities for cybersecurity practitioners to research and train on advanced security evaluation techniques.
- To build up local product evaluation expertise, NICE will support training courses and internships for students and professionals to learn more about security evaluation methodologies and certification processes.

https://go.gov.sg/wo0buv

CSA's Cybersecurity Certification Guide

Grow our cybersecurity market

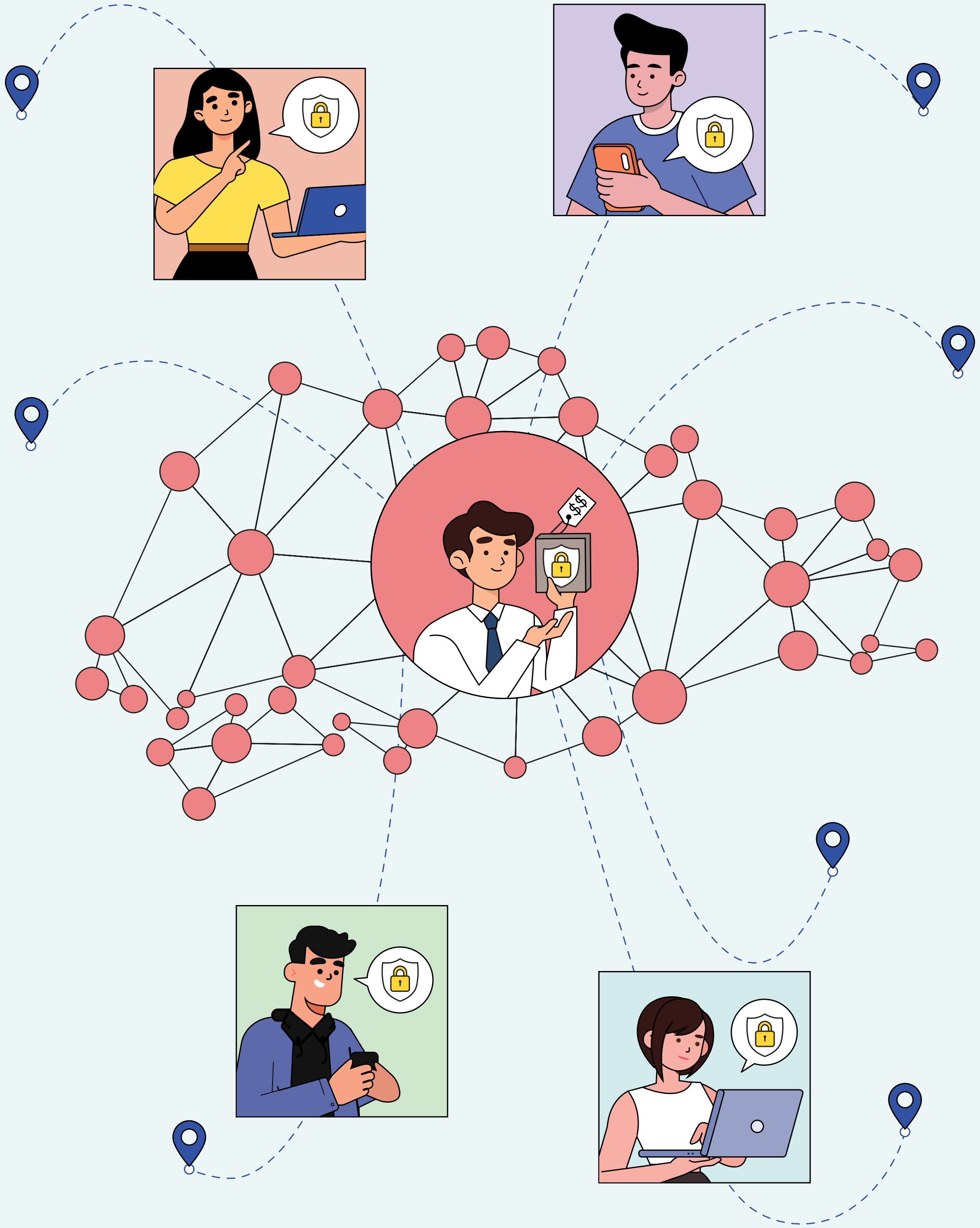
We seek to grow the market for Made-in-Singapore cybersecurity products and services. We will do so by supporting user adoption to drive demand for cybersecurity solutions. We will also encourage Singapore-based companies to internationalise and export their products and services.

Encourage adoption of cybersecurity solutions

Supporting user adoption helps build a steady demand for cybersecurity solutions. The Government will encourage user adoption by making cybersecurity solutions more accessible. Today, SMEs are already eligible for subsidised pre-approved cybersecurity solutions under the SMEs Go Digital programme. For larger enterprises and organisations with specific cybersecurity needs, the Government will play a facilitative role to match supply with demand for more sophisticated solutions, given that end-users may not always be familiar with the wide range of cybersecurity solutions in the market.

Internationalise our cybersecurity companies

Local companies should not limit themselves to the Singapore market and look to expand into new markets to capture the growing global and regional demand for cybersecurity products and services. The Government is looking to support promising local cybersecurity companies to expand overseas and export Made-in-Singapore solutions. For instance, the Government will curate, organise, and support these cyber companies in profiling their solutions internationally.



CHAPTER 5

GROW A ROBUST CYBER TALENT PIPELINE

GOAL

Develop and sustain a strong cybersecurity workforce to meet our security and economic needs

The successful execution of our cybersecurity strategy ultimately hinges on our people and talent.

The breadth and depth of cybersecurity responsibilities for the Government, enterprises, and organisations will continue to grow. Amidst an ever-evolving technological landscape, we will need to groom new talent and upskill existing professionals to achieve the objectives discussed in the earlier chapters.

It is therefore critical for Singapore to strengthen the cybersecurity talent pipeline. We can do so by leveraging our strong education system to grow a skilled cybersecurity workforce. This will enhance Singapore's competitive advantage, especially amidst a global shortage of cybersecurity professionals.

WHAT'S NEW?

Strategy 2016 had sought to ensure an adequate and well-trained cybersecurity workforce in light of growing demand for cybersecurity manpower. We have made good progress. Based on the 2020 Infocomm Media Development Authority (IMDA) Survey on Infocomm Media Manpower, there were more than 10,700 cybersecurity professionals in Singapore in 2020, up from around 6,000 cybersecurity professionals in 2018.

In Strategy 2021, we will take further steps to:

▶ Move upstream to engage talent

We want to reach out to the young to develop their interest and cyber skills, and encourage more youths to pursue a career in cybersecurity.

▶ Strengthen our cyber workforce

We want to make sure that cybersecurity professionals have access to training resources and opportunities to keep pace with the ever-evolving cyber threat landscape.

Industry partners, IHLs, and professional associations are key partners to achieve these goals. Building on Singapore's strong education system, the Government will work with all stakeholders to **support youths, women, and mid-career professionals to pursue a cybersecurity career**. To ensure that our cybersecurity workforce is well equipped with the requisite skills and knowledge, we will **create an upskilling culture** and **foster a dynamic sector with strong professional communities**.

Support youths, women, and mid-career professionals to pursue a cybersecurity career

The growth of a capable and competent workforce is sustained by attractive career prospects and a respected professional status. We will build on existing initiatives to attract more talented individuals to the cybersecurity profession. We will also nurture young Singaporeans' interest in cybersecurity and engage under-represented groups in the cybersecurity profession.

Interest and enable youths to pursue cyber as a career

We seek to attract promising youths to the cybersecurity industry to build a pipeline of local talents for the longer-term. The Government will work closely with schools and other partners to engage youths through cybersecurity bootcamps, competitions, learning journeys, and career mentoring. In addition, the Government will equip school teachers and career counsellors with knowledge of the cybersecurity sector to guide students in their career choices under the SG Cyber Educators initiative. Selected male youth with aptitude and interest for cybersecurity can also serve their National Service under the Cyber Work-Learn scheme. This will further enhance the talent pipeline with continued skills development and hands-on experience.

SG Cyber Youth

SG Cyber Youth is a national programme that guides youths in their cybersecurity journey, with support from the academia, community, and industry. A key initiative is the Youth Cyber Exploration Programme that introduces pre-tertiary students to the fundamentals of cybersecurity and cultivates their interest in a cybersecurity career. The Cybersecurity Career Mentoring Programme (CCMP) also provides career guidance and support from industry mentors. Other initiatives include the Student Volunteer & Recognition Programme (SVRP) and Cybersecurity Learning Journeys. Through the various programmes, we will identify a pool of local youths with exceptional cybersecurity talent, who will be groomed under the SG Cyber Olympians programme through cyber sparring sessions, deeper training, and international competitions.

SG Cyber Youth

https://go.gov.sg/opncee

Join the mailing list:

https://go.gov.sg/ot74un

Attract diverse talent

Apart from youths, the Government is also looking to attract more women and mid-career professionals from adjacent fields to join the cybersecurity industry. We will work closely with industry and international partners to encourage girls to take up cybersecurity education programmes and inspire women to take on cybersecurity roles. We will also encourage mid-career professionals to join the cybersecurity sector by leveraging professional conversion programmes such as the Cyber Security Associates and Technologists programme.

SG Cyber Women

Women in Cyber event at SICW 2020

Women remain under-represented in the cybersecurity profession. In partnership with industry and the local cybersecurity community, CSA launched SG Cyber Women, a targeted initiative to encourage more women to pursue a career in cybersecurity.

Past programmes that have been organised as part of SG Cyber Women include the Capture-The-Flag for Girls competition, Ladies in Cyber mentorship programme and technical workshops. In 2020, CSA also launched the SG Cyber Women X Series, a series of virtual events in celebration of International Women in Cyber Day. Women of all ages can participate in these events to find out more about cybersecurity or deepen their skills to further their career.

SG Cyber Women

https://go.gov.sg/rzkrbw

Create an upskilling culture for a globally competitive workforce

A highly-skilled workforce is crucial to grow the cybersecurity industry, which will be a key sector in Singapore's economy and digital future. Apart from attracting new talent to the profession, the Government will partner the industry and IHLs to enhance career pathways and facilitate the development of deep skills. The Government will also raise, train, and sustain cybersecurity professionals in the public sector.

Enhance career pathways and facilitate development of deep skills

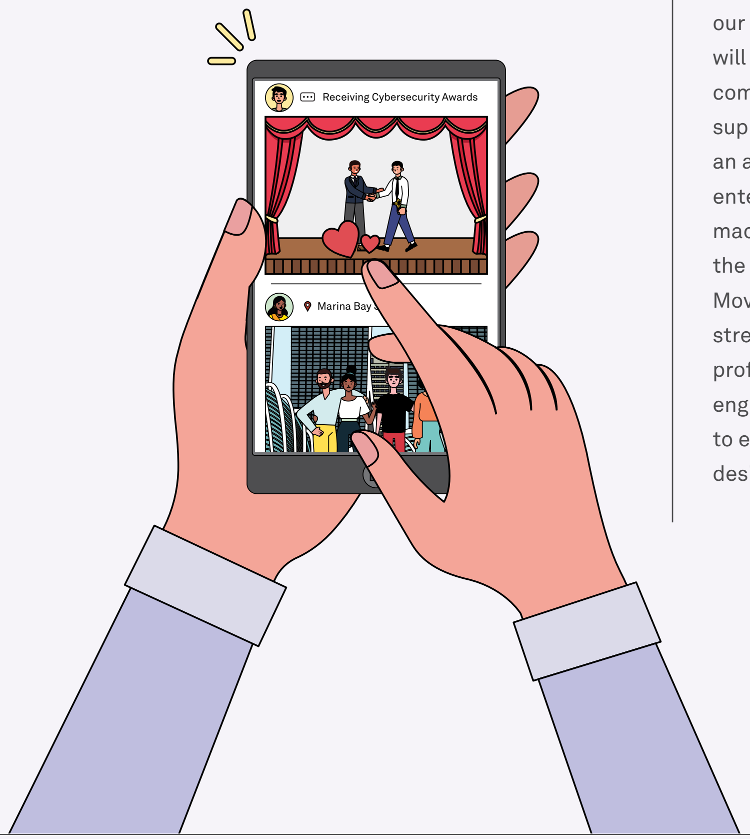
The Government will facilitate and guide our professionals by developing good career pathways and skills training frameworks. For example, the Government launched the Skills Framework for ICT and the OT Cybersecurity Competency Framework, which are tools that enterprises can leverage to enhance career pathways for cybersecurity professionals in their organisation. We will also improve access to training and networking opportunities for cybersecurity professionals. Today, professionals can already tap on training grants to upgrade their skills or join programmes such as the SG Cyber Leaders programme to network with current and future cybersecurity leaders.

Raise, train, and sustain cybersecurity professionals in the public sector

The Government will develop good career pathways for cybersecurity professionals in the public sector. For example, CSA developed the Cyber Security Development Programme to train a common pool of cybersecurity experts for the public sector. Upon completion of the Programme, participants can choose to pursue a career within the public service or enter the private sector. CSA also set up the CSA Academy, which provides cybersecurity professionals in the Government and CII sectors with niche courses not readily available in the training market.

Foster a dynamic sector with strong professional communities

We have observed a marked improvement in the standing of cybersecurity professionals and the emergence of a strong common identity. To build stronger communities of practice and foster trust within the profession, the Government will work closely with industry associations to further recognise the achievements and contributions of our cybersecurity community.



Support our cybersecurity community and recognise excellence

The cybersecurity industry, professional bodies, and academia are key stakeholders in Singapore's journey to grow a strong cyber workforce. Our industry and community partners often organise community events, workshops, conferences, and programmes that help strengthen the talent pipeline and develop our professionals. The Government will support and recognise these community efforts. For example, CSA supports the Cybersecurity Awards, an annual event that recognises enterprises and individuals who have made significant contributions to the local cybersecurity ecosystem. Moving forward, the Government will strengthen engagement with other professional bodies such as those for engineers and software developers, to encourage them to build secure-by-design products and services.

CONCLUSION

The Singapore Cybersecurity Strategy 2021 serves as a blueprint for Singapore and Singaporeans to secure our Smart Nation, amidst an ever-evolving cyber threat landscape and emerging digital technologies. Cybersecurity is our collective responsibility. With everyone doing their part, we can create an open, secure, stable, accessible, peaceful, and interoperable digital environment, and reap the opportunities that digitalisation has to offer.

TERM	DEFINITION
Artificial Intelligence (AI)	Refers to the study and use of intelligent machines to mimic human action and thought.
Attack Surface	Refers to all vulnerable resources of a system, or the sum of the points through which an attacker could try to enter an environment.
Cloud	A model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Critical Information Infrastructure (CII)	The computer or computer system necessary for the continuous delivery of an essential service, which the loss or compromise thereof will have a debilitating effect on the availability of essential services in Singapore.
Cybercrime	Criminal acts related to the use of computers such as gaining unauthorised access to a computer to view, modify or destroy its data.
Cyberspace	The complex environment resulting from the interaction of people, software and services on the Internet by means of technological devices and networks connected to it, which does not exist in any physical form. Singapore's cyberspace includes domain names with ".SG" or Singapore-mentions, Internet Protocol (IP) addresses used in Singapore, and Internet Service Providers (ISPs) located here.
Domain Name System (DNS)	Refers to the system used to translate readable domain names to IP addresses.
Edge Computing	Refers to the practice of capturing, processing, and analysing data near the source of data.
Internet of Things (IoT)	The vast network of everyday objects, such as baby monitors, printers, televisions, and autonomous vehicles, that are connected to the Internet.
Operational Technology (OT)	Programmable systems or devices that interact with the physical environment or manage devices that interact with the physical environment. Examples include industrial control systems and building management systems.
Penetration Testing	An authorised simulated attack on a system to evaluate the efficacy of the security measures in place.
Quantum Technologies	A class of technologies that works by using the principles of quantum mechanics (the physics of sub-atomic particles). Examples of quantum technologies include quantum computing and cryptography.
Ransomware	Malware that encrypts files on a victim's device, rendering them unusable until a ransom is paid, usually in the form of Bitcoin or other cryptocurrencies. It may spread through phishing e-mails that contain malicious attachments or links, or malicious pop-ups that appear when users access unsafe websites.
Secure-by-Design	An approach to software and hardware development that seeks to minimise system vulnerabilities and reduce the attack surface, by designing and building in security at every development phase.
Vulnerability	A weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.
Zero-Trust	A security framework requiring all end-users, whether in or outside the organisation's network, to be authenticated, authorised, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Contact Details

If you have any feedback on this publication, or wish to find out more about Singapore's efforts in cybersecurity, please visit the following websites or contact us:

Cyber Security Agency of Singapore

Website:

www.csa.gov.sg

General enquiries/feedback:

contact@csa.gov.sg

GoSafeOnline

Website:

www.csa.gov.sg/gosafeonline

If you wish to report a cybersecurity incident, please contact:

SingCERT

Website:

www.csa.gov.sg/singcert/reporting

If you wish to seek scam-related advice:

ScamAlert

Contact anti-scam helpline:

1800 722 6688

Visit ScamAlert website:

www.scamalert.sg

CSA
SINGAPORE