SINGAPORE'S SAFER CYBERSPACE MASTERPLAN 2020

Acknowledgements

We would like to thank the following groups, individuals and agencies for their valuable input and support over the course of developing the Safer Cyberspace Masterplan:

- The Association of Information Security Professionals Executive Committee
- The Cyber Security Awareness Alliance
- The SGTech Cybersecurity Chapter Executive Committee
- Mr. Benjamin Ang, S. Rajaratnam School of International Studies (RSIS) Centre of Excellence for National Security
- Associate Professor David Lo, Singapore Management University School of Information Systems
- Professor Lam Kwok Yan, Nanyang Technological University School of Computer Science and Engineering
- The Infocomm Media Development Authority (IMDA), the Ministry of Education (MOE), the Singapore Police Force (SPF) and the Smart Nation and Digital Government Group (SNDGG)

Table of Contents

Foreword

Digitalisation has changed the way we work, learn, transact and stay connected. The COVID-19 pandemic has accelerated the scale, scope, and speed of digitalisation. There are tremendous opportunities as we move towards being a Smart Nation and Digital Economy.

However, an increasingly digital way of life also increases cyber risks. Malicious actors will have a wider attack surface to exploit digital assets and data. Cybersecurity is a critical enabler of our digital economy, giving our people the confidence to navigate and pursue the opportunities. Now, more than ever, we must make concerted efforts to ensure a safe and secure digital infrastructure for Singaporeans and businesses.

The Safer Cyberspace Masterplan represents the Government's blueprint for the medium term to better protect Singapore and Singaporeans in the digital domain. It focuses on upstream measures to secure Singapore's core digital infrastructure, safeguard our activities in cyberspace, and empower our population to adopt better cyber hygiene.

Everyone has a part to play in creating a safer and more secure cyberspace. The Government will take the lead, but a collective effort from the community, enterprises and individuals will be critical to raise Singapore's overall cybersecurity posture. That is why every action counts, whether it is the individual who adopts good cyber hygiene, or a company who makes the effort to better secure their assets and data in cyberspace, using the resources outlined in this Masterplan.

In an increasingly interconnected world, a strong and proactive cybersecurity approach is an essential investment that will allow us to reap the dividends of the digital economy. Together, we can realise our vision of a Safer Cyberspace for Singapore and Singaporeans — one that helps to boost Singapore's connectivity, promotes businesses' competitive advantage, and improves the lives and livelihoods of Singaporeans.

S Iswaran
Minister-in-charge of Cybersecurity
and Minister for Communications and Information

EXECUTIVE SUMMARY

Digitalisation has changed the way we live, work and play; it also brings about vast opportunities for us to seize.

As Singapore embarks on its digital transformation toward a Smart Nation and Digital Economy, Singaporeans and our enterprises will also face increasing cyber threats as more of our citizens and businesses go online. Cybersecurity will be a critical enabler of our push toward digitalisation. Without robust cybersecurity in place, our systems and networks remain open and vulnerable for malicious threat actors to exploit our digital assets and data.

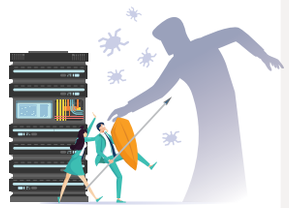
To this end, the Safer Cyberspace Masterplan aims to raise the general level of cybersecurity in Singapore, for individual users, communities, enterprises, and organisations. It comprises the following three thrusts:

A

Securing our core digital infrastructure

B

Safeguarding our cyberspace activities



C

Empowering our cyber-savvy population

Our digital infrastructure forms the technology backbone of how users access the Internet (the "pipes"), our online activities represent the traffic that flows through those pipes, and our population are the end-users whom we wish to protect. Taken together, these three thrusts are mutually reinforcing in contributing to a safer cyberspace as our citizens and businesses increasingly shift their activities online. What they mean for Singapore and Singaporeans are that:

Singaporeans are protected from most online harm ever reaching us.

If threats come through our defences, we know about them early and can take action to prevent damage. This entails businesses making use of readily available resources to take actionable steps to protect themselves.

Singaporeans can live, work and transact in the digital domain securely, having taken steps to protect themselves online.

Everyone has a role to play in the cybersecurity of our shared digital space.

The Government will:

Safeguard the security and resilience of Singapore's 5G networks, working together with our Mobile Network Operators (pages 20-21).

Enable the swift detection of and response to malicious cyber activities, to prevent them from reaching end-users as far as possible. We will do so by leveraging human-AI collaboration and also monitoring global developments in IoT threats and vulnerabilities (pages 32-33, 36).

Individuals can strengthen their cybersecurity posture, by:

Being mindful of the increasing frequency and sophistication of cyber threats as more aspects of our lives go online (pages 46-49).

Adopting good cyber hygiene practices in our day-to-day online activities (page 47):

- Use strong passwords and enable Two-Factor Authentication
- Use an anti-virus software
- Update software as soon as possible
- Spot signs of phishing

Choosing to buy IoT devices that are more secure at a higher Cybersecurity Labelling Scheme tier (pages 26-27).

The Government will take the lead to implement and roll out initiatives at the national level to protect our digital infrastructure. However, that in itself is not sufficient to safeguard all of us against the wide range of cyber threats. Enterprises and organisations, and individuals, can leverage the initiatives in the Masterplan to better protect themselves. The initiatives in the Masterplan are specifically aimed at increasing the adoption of security-by-design amongst enterprises and organisations, and enhancing cybersecurity awareness and good cyber hygiene practices amongst end users.

Enterprises and organisations can strengthen their cybersecurity posture, by:

Leveraging the cybersecurity toolkits and resources aimed at enhancing awareness amongst business leaders, IT teams, and general employees of the cyber risks faced by enterprises and organisations (pages 44-45).

Protecting the enterprise or organisation's data and networks:

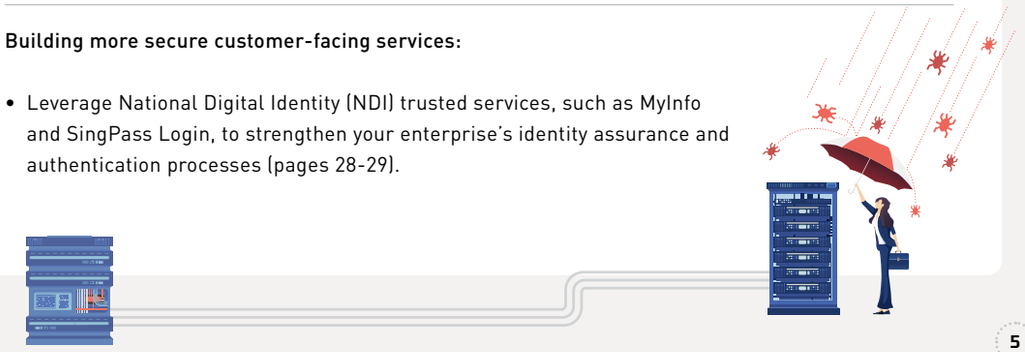
- Use secure Cloud services with peace of mind that your data and systems on the Cloud are adequately protected (page 24).
- Adopt the Security-as-a-Service cyber solution that creates a zero-trust cyber environment against malicious applications and software, and implements essential cybersecurity principles in your computers (pages 40-41).
- Assess your enterprise or organisation's domain, connectivity and email health using the Internet Cyber Hygiene Portal (pages 38-39).

Achieving recognition for the level of cyber hygiene of your enterprise or organisation:

- Apply for the SG Cyber Safe Trustmark to demonstrate that your enterprise or organisation has put in place the pre-determined cybersecurity measures (pages 50-51).

Building more secure customer-facing services:

- Leverage National Digital Identity (NDI) trusted services, such as MyInfo and SingPass Login, to strengthen your enterprise's identity assurance and authentication processes (pages 28-29).



CHAPTER 1

A Safer Cyberspace for Singapore and Singaporeans

Why do we need a Safer Cyberspace Masterplan?

The Singapore Government is committed to enable a Smart Nation and harness digital technology to stay ahead as a global city and to improve lives and livelihoods for all. As we embrace digital technology, it is apparent that the same technology provides malicious actors with new avenues to conduct their activities.

> "As the digital economy grows in scale and complexity, cybersecurity becomes of utmost importance to provide the much needed and requisite assurance and trust in digital technologies."
>
> S Iswaran, Minister-in-charge of Cybersecurity, at the ASEAN Ministerial Conference on Cybersecurity 2019

In 2016, the Government launched the Singapore Cybersecurity Strategy with four Pillars: to build a resilient infrastructure, create a safer cyberspace, develop a vibrant cybersecurity ecosystem, and strengthen international partnerships. The Safer Cyberspace Masterplan builds on the 2016 Strategy to articulate a more detailed plan toward **Pillar 2 — the Creation of a Safer Cyberspace in Singapore.**

This Masterplan aims to **raise the general level of cybersecurity in Singapore, for individual users, communities, enterprises, and organisations.** The Government has developed the key thrusts of the Masterplan in consultation with the cybersecurity industry and academia, and incorporated many of their useful ideas toward our collective purpose to create a Safer Cyberspace for Singapore and Singaporeans. While there may be some similarities with the measures that have been put in place for Critical Information Infrastructure (CII) designated under the Cybersecurity Act 2018 that support essential services, the Safer Cyberspace Masterplan seeks to address a different class of users and system owners from CIIs, and hence should be seen as separate from the CII regulatory regime.

Prevention — Better than cure?

With technology touching all parts of our lives today, cybercriminals have many opportunities to make a quick buck. What if we could make it more difficult for threat actors to commit malicious cyber activities in the first place, and can swiftly detect and respond to an incident after it happens? This is the approach of the Masterplan, which focuses on upstream measures to prevent and detect malicious cyber activities.

An analogy from the physical world parallel to cyberspace would be preventive healthcare. Doctors advocate a healthy lifestyle and regular health screening in order to nip diseases in the bud before they become severe. The cyber equivalent of preventive health needs to be implemented, to better protect Singapore and Singaporeans in the digital domain. While there will inevitably be events that we cannot foresee in the cyber and the health domains, taking early preventive measures will avoid a vast majority of unpleasant and costly events from happening later on. In addition, just as how we are encouraged to go for regular health check-ups to detect the onset of health conditions early, we want to adopt the cyber equivalent of detecting and responding to malicious cyber activities swiftly when they arise.

The analogy further extends to the roles of the Government, community, enterprises and the public. To encourage good preventive health habits, the Government puts in place community exercise corners and works with the food industry to reduce the amount of sugar in our food products, to make it easier for individuals to adopt a healthy lifestyle. Yet individuals continue to bear the responsibility to exercise and consume food and beverages with healthier food labels.

This is parallel to cybersecurity — the Government will put in place upstream measures to make it more difficult for actors to conduct malicious cyber activities on us, but the community, enterprises and individuals must continue to take personal responsibility for their safety and security in the digital domain.

Singapore is highly dependent on the digital domain for business and our daily lives

98%

Households with Internet access[1]

6H 48M Daily time spent online[2]

94% Business Broadband Adoption[3]

SGD 37 BILLION
(USD 27 BILLION)
Singapore's estimated Internet Economy in 2025[4]

While the initiatives in the Masterplan will make our cyberspace more secure over time, it is unrealistic to expect that all malicious cyber activities can be prevented. With the contours of cyberspace constantly changing, new threats will emerge, and unknown vulnerabilities will be found. The Government will play its part to support a safe and secure cyberspace, but the community, enterprises and individuals need to remain vigilant in cyberspace and continue adopting practices to keep themselves safe and secure online. Ensuring the cybersecurity of our digital assets and data is our collective responsibility.

Individuals and businesses remain exposed to malicious cyber activities

28% of Singaporeans surveyed said they were victim to at least one cyber incident in 2019[5]

Almost 2 in 5 of all cyber incidents in Singapore target SMEs[6]

SGD 18.9 MILLION
(USD 13.8 MILLION)
is the estimated loss to a large enterprise from a cyber-attack. The average cost to a medium-sized enterprise is $26,000.[7]

58% of enterprises that use the Internet for work have no cybersecurity measures[8]

1 Infocomm Media Development Authority. "Annual Survey on Infocomm Usage in Households and by Individuals for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/research-and-statistics/survey-report/2019-hh-public-report_09032020.pdf
2 We are Social. "Digital 2020 Singapore", 12 February 2020, https://wearesocial.com/sg/digital-2020/singapore
3 Infocomm Media Development Authority. "Annual Survey on Infocomm Usage by Enterprises for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/industry-development/fact-and-figures/infocomm-usage-business/infocomm-usage-survey-public-report-2019.pdf
4 Google & Temasek / Bain. "e-Conomy SEA 2019", 3 Oct 2019. https://blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf
5 Cyber Security Agency of Singapore. "CSA Public Awareness Survey 2019", 21 August 2020, https://www.csa.gov.sg/news/press-releases/csa-public-awareness-survey-2019
6 Cyber Security Agency of Singapore. "Singapore Cyber Landscape 2017", 19 June 2018, https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018
7 Frost Sullivan. "Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World", 17 May 2018, https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/
8 Infocomm Media Development Authority. "Annual Survey on Infocomm Usage by Enterprises for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/industry-development/fact-and-figures/infocomm-usage-business/infocomm-usage-survey-public-report-2019.pdf

WHO ARE WE DEFENDING AND WHAT ARE WE DEFENDING AGAINST?

Since the inception of the Cybersecurity Act in 2018, we have made significant progress in ensuring that our CIIs that support essential services are robustly defended. We are focusing our attention now on developing a more detailed and concrete plan to ensure that other users of our cyberspace are sufficiently defended. These users include ordinary users, enterprises (especially small and medium ones), and organisations. For many of them, the Internet is an inextricable part of their lives and work, but more can and should be done to help ensure that their experience on the Internet is a safer and more secure one. If they are unable to protect or defend themselves against cyber-attacks, many of them may suffer distress or even financial loss. While CSA has conducted extensive outreach and engagement efforts in the past, our survey results suggest that this group remains vulnerable to cyber threats.

In addition, as the level of digital activity increases, the types of malicious cyber threat actors and the methods that they employ have also become more diverse and sophisticated. These actors deploy a variety of tactics to seize control of devices, gain access to personal data, or in severe cases, cause disruption of services. These range from sending phishing e-mails, directing individuals to malicious websites, to deceiving users to download malware-laden software.

Cyber Threat Actors Targeting Singapore and their Motivations

Advanced Persistent Threats (APTs)

APTs operate stealthily and with sophistication, often hiding in networks for prolonged periods to plan their targeted attacks. APTs — which may refer to the type of attack, or the threat actor or group — are also often state-sponsored. Their motivations include disruption of services and operations, espionage to gather privileged information, and financial gain.

Hacktivists

Hacktivism involves hacking (i.e. breaking into a computer system) and defacing webpages to promote a political or ideological message. Online activism through hacking has become an increasingly attractive alternative to conducting physical street protests, as the Internet affords hacktivists anonymity and wider reach.

Cybercriminals

This group of threat actors typically adopt social engineering techniques to lure their victims, predominantly for financial gain. Cases include online cheating, cyber extortion and unauthorised access to computer material and data. The anonymity provided by the Internet and borderless nature of cyberspace allow cybercriminals to operate freely, and law enforcement agencies need to work closely with the public to collectively tackle the scourge of cybercrime.

Methods used by Threat Actors that Affect Individuals and Businesses

Phishing

Phishing remains the most frequently employed tactic. Malicious actors pose as a legitimate institution to lure individuals to give away confidential, and often valuable, information.

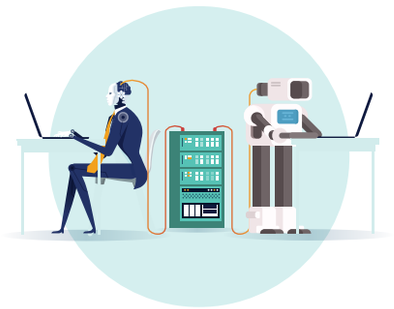
- 47,500 phishing URLs with a Singapore-link were detected in 2019, and 70% of incidents reported to the Singapore Computer Emergency Response Team (SingCERT) by Small and Medium Enterprises (SMEs) and individuals occurred through phishing attacks.

- In Singapore, the most commonly spoofed websites of Government organisations included the Immigration & Checkpoints Authority (ICA), Ministry of Manpower (MOM) and Singapore Police Force (SPF). To mitigate this, the Government has made it easier for members of public to identify potential fraudulent websites by moving most Government websites to the .gov.sg domain, making it more difficult for malicious actors to spoof legitimate Government websites.

Ransomware

Ransomware prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

- SingCERT received 35 reports of ransomware cases in 2019, an increase from 21 in 2018. Systems across various industries including gaming, travel and tourism, manufacturing, and hardware, were affected.



Botnets

A botnet (or robot network) consists of a network of Internet-connected devices infected with malicious software (botnet drones). The botnet drone is remotely-controlled by a Command & Control server (C&C Server). Botnets can be used to disrupt online services, send spam or access the computing resources of infected devices.

- SingCERT detected about 530 C&C servers in Singapore in 2019. On a daily basis, SingCERT observed an average of 2,300 botnet drones.

Cyber threats in numbers[9]

Cybercrime cases reported in 2019:

9,430
(close to 26 cases daily on average)

Cybercrime accounted for

of overall crime in 2019.

2,300
compromised computers (botnet drones) with Singapore addresses observed daily

873
Singapore-linked website defacements were detected in 2019.

[9] Cyber Security Agency of Singapore. "Singapore Cyber Landscape 2019", 26 June 2020, https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2019

Case Study — Incident in E-Commerce Sector

In late-2019, customers of a local online fashion retailer were informed that hackers had tried to harvest their personal information by injecting malicious code into the retailer's e-commerce website.

Investigations revealed that the injected malicious code allowed a fake form to overlay the genuine web form used for collecting personal information from the retailer's customers. Personal information that was subsequently stolen included the customers' first and last names, e-mail addresses, shipping addresses, order details, payment type, and credit card information.

Follow-up Action

Upon discovering the data breach, the retailer alerted the Singapore Police Force and Personal Data Protection Commission. It also worked with cybersecurity experts to remove the malicious code from the affected website, and implemented measures to secure their systems. These measures included enforcing two-factor authentication (2FA) for back-end access, password resets for all user accounts, and further digital forensic analysis. Updates about the mitigation measures taken were also circulated to the retailer's customers.

Businesses risk tarnishing their reputations and losing consumer confidence if they do not take privacy issues seriously, or fail to protect their platforms with robust cybersecurity measures. They should ensure that their websites and databases are secure and regularly patched.

What does this Masterplan entail?

The Masterplan comprises the following three thrusts: (a) Securing our core digital infrastructure, (b) Safeguarding our cyberspace activities, and (c) Empowering our cyber-savvy population. Our digital infrastructure forms the technology backbone of how users access the internet (the "pipes"), our online activities represent the traffic that flows through those pipes, and our population are the end-users whom we wish to protect; taken together, these three thrusts are mutually reinforcing in contributing to a safer cyberspace. The aim of these three thrusts are:

Securing our Core Digital Infrastructure

Desired Outcome:

Make Internet architecture, user devices and endpoints, and applications, secure by default.

What it means for Singapore and Singaporeans:

Singaporeans are protected from most online harm ever reaching us.

Safeguarding our Cyberspace Activities

Desired Outcome:

Discover malicious cyber activities early through active threat detection and analysis, and the provision of self-help tools and solutions for cyberspace users.

What it means for Singapore and Singaporeans:

If threats come through our defences, we know about them early and can take action to prevent damage. This entails businesses making use of readily available resources to take actionable steps to protect themselves.

Empowering our Cyber-Savvy Population

Desired Outcome:

Enhance awareness and adoption of cybersecurity measures to keep ourselves safe and secure in cyberspace.

What it means for Singapore and Singaporeans:

Singaporeans can live, work and transact in the digital domain securely, having taken steps to protect themselves online.

The Masterplan also outlines 11 initiatives under these three thrusts that serve as examples of how the Masterplan can help to better safeguard and protect our cyberspace, and mitigate the impact through swift detection and response.

Overview of the Safer Cyberspace Masterplan

3 STRATEGIC THRUSTS

7 FOCUS AREAS

11 KEY INITIATIVES

Securing our Core Digital Infrastructure

Protecting the Internet Architecture in Singapore

Securing User Devices and Endpoints

Safeguarding Enterprise Applications

- Secure Singapore's 5G networks
- Strengthen cybersecurity of Cloud services
- Cybersecurity Labelling Scheme
- Leverage National Digital Identity trusted services for identity assurance and authentication

Safeguarding our Cyberspace Activities

National Detection and Analysis of Malicious Cyber Activities

Enabling Enterprises to Protect Themselves from Cyber Threats

- Human-AI collaboration for swift detection and response
- Early detection and response to impending IoT attacks
- Internet Cyber Hygiene Portal
- Security-as-a-Service cyber solution

Empowering our Cyber-Savvy Population

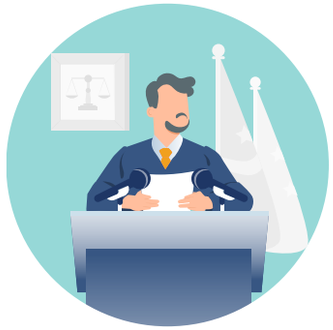
Raising Awareness and Changing Attitudes on Cybersecurity

Enhancing Cyber Adoption

- Cybersecurity resources and toolkits for enterprises
- Raise community awareness of cybersecurity
- 5G Cyber Safe Trustmark

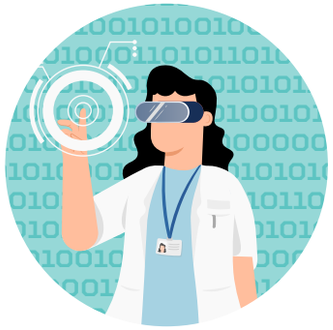
How does the Masterplan apply to Singaporeans and enterprises?

Everyone has a role to play in cybersecurity:



The Government

will drive the efforts to develop a high standard of online security, partnering with the cybersecurity industry, academia, enterprises and organisations, and individuals.



Cybersecurity industry and academia

will develop the innovative cybersecurity solutions and products, through research and development, to better secure our cyberspace.

Enterprises and organisations

must protect their systems by building cyber defence capabilities and putting in place digital risk management measures.

Individuals

should practice good cyber hygiene and remain vigilant online.

The initiatives in this Masterplan are targeted for implementation from 2021-2023. It will be reviewed regularly and new initiatives will be added as necessary to keep up with the prevailing cyber threat landscape.

" Cybersecurity has long passed the point where it is purely a technical issue. It has become a business continuity issue, a business strategy issue. It has floated up to the top of the agenda of the Board."

Dr Janil Puthucheary, Senior Minister of State-in-charge of Cybersecurity, at the Singapore International Cyber Week 2019

CHAPTER 2

Securing Our Core Digital Infrastructure

The first strategic thrust of the Safer Cyberspace Masterplan aims to **secure our core digital infrastructure by tackling known cybersecurity vulnerabilities upfront, and achieve security-by-design.** Exposure to such vulnerabilities will be minimised for the end-user connected to the Internet in Singapore, simply because measures have been put in place at the national level to mitigate the known vulnerabilities, or security flaws have been addressed in the design of the architecture — all before end-users can be exposed to them.

This infrastructure layer defends Singapore's cyberspace right at the outset, by minimising vulnerabilities in our **Internet architecture, devices and endpoints**, and **enterprise applications**. New vulnerabilities constantly arise, and infrastructural protection is not fool-proof. The other two layers — safeguarding cyberspace activities and empowering a cyber-savvy population — in Chapters 3 and 4 augment our efforts on this front.

Protecting the Internet Architecture in Singapore

This involves protecting our next-generation telecommunications networks and implementing security measures to stop threats at the edge of Singapore's cyberspace:

1 Secure Singapore's 5G networks against cyber-attacks

What is the need?

5G is touted to revolutionise info-communications technology. It promises to provide up to 100 times more bandwidth — at ultra-low latency — than the current 4G mobile broadband plans that are currently offered to mobile subscribers. These improvements will change how we work and play — for example, accelerating the adoption of Virtual Reality use-cases among businesses and consumers alike, and enabling other new technologies such as autonomous vehicles. 5G will also be a key enabler of Industry 4.0, transforming manufacturing and production through remote and automated command and control of the factory floor.

The anticipated high reliance on, and connectivity of, 5G could cause massive service disruption and significant impact to businesses and the public if there are service outages. With the large amount of data envisioned to traverse through 5G networks, it would also be an attractive target for malicious actors to siphon confidential data. As such, it is critical that our 5G systems are secure and resilient against such cybersecurity threats.

Safeguarding our next-generation telecommunications networks

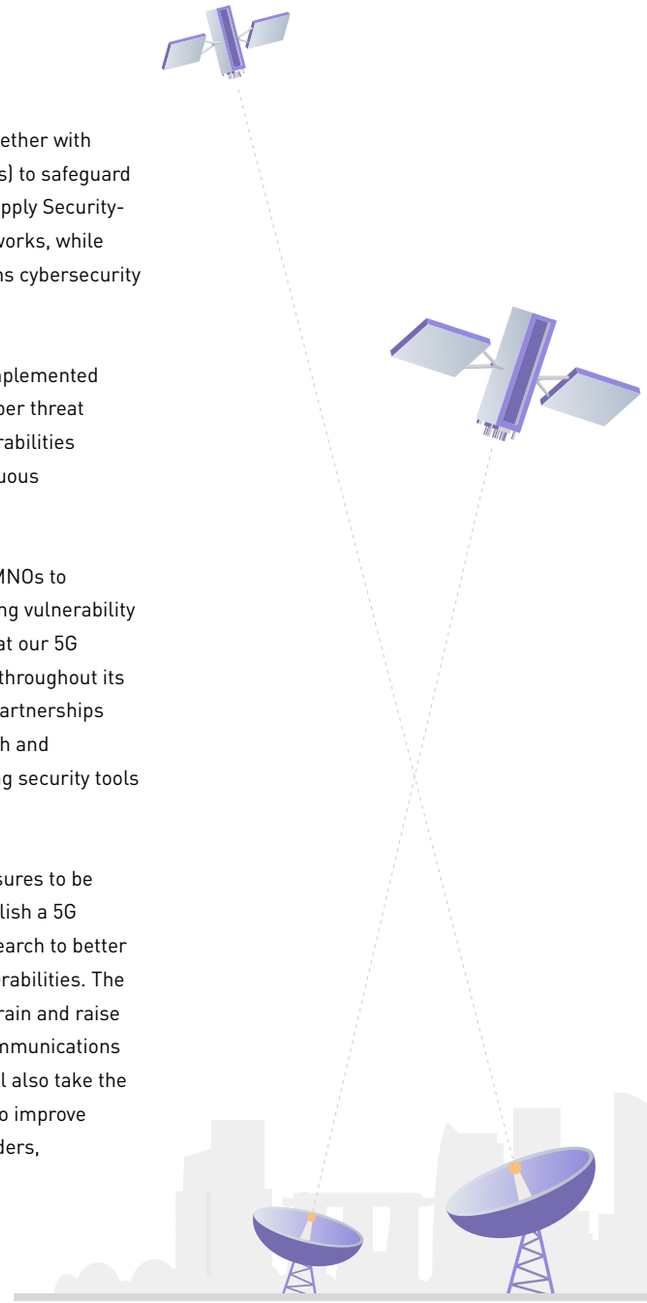
What will we put in place?

The Infocomm Media Development Authority (IMDA), together with CSA, will work with the mobile network operators (MNOs) to safeguard the security and resilience of our 5G networks. We will apply Security-by-Design[10] principles in developing Singapore's 5G networks, while concurrently building up world-class telecommunications cybersecurity capabilities locally to handle 5G cybersecurity threats.

In addition to ensuring that 5G security measures are implemented from the get-go, the Government recognises that the cyber threat landscape evolves over time, and new threats and vulnerabilities will inevitably arise. There is therefore a need for continuous security assurance.

To this end, IMDA together with CSA will work with the MNOs to enhance the 5G cybersecurity posture, such as conducting vulnerability assessments[11] and threat hunting[12] work, and ensure that our 5G networks are secure against new and emerging threats throughout its operational lifecycle. This will involve developing close partnerships with the cybersecurity industry and academia to research and implement cutting edge solutions to complement existing security tools designed for 5G systems.

As part of the ongoing cybersecurity enhancement measures to be adopted for the 5G networks, IMDA and MNOs will establish a 5G Security Programme for technology exploration and research to better protect our 5G networks against cyber threats and vulnerabilities. The Programme will also provide a testbed environment to train and raise the 5G cybersecurity skills and knowledge of our telecommunications cybersecurity professionals. IMDA together with CSA will also take the lead to conduct cybersecurity exercises with the MNOs to improve the incident response and coordination among stakeholders, in the event of a cyber-attack on 5G systems.



[10] Security-by-Design refers to the 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.
[11] Vulnerability assessment refers to the process of identifying, quantifying and prioritising the vulnerabilities of a system, after which vulnerabilities are addressed to prevent exploitation.
[12] Threat hunting is the process to proactively and iteratively search for cyber threats through networks that may have evaded existing security measures.

Feature: DNSSEC

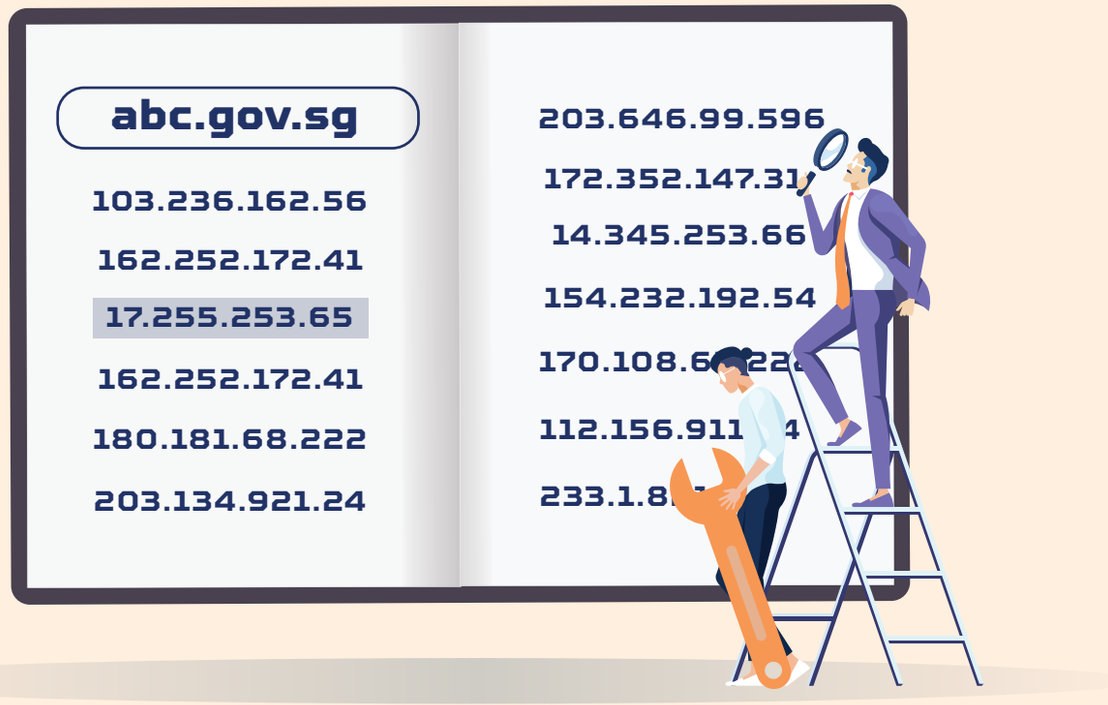
Strengthening security of our Internet infrastructure through Domain Name System Security Extension (DNSSEC) measures

As we work toward protecting our future 5G networks against cyber threats, it is important to also address existing security gaps in our Internet infrastructure today. One example is the Domain Name System (DNS).

The DNS is the naming system for the Internet. It translates readable domain names (like www.google.com) to Internet Protocol (IP) addresses, so that Web browsers can access Internet resources. However, the DNS today has security vulnerabilities that allows traffic meant for legitimate servers to be diverted to bogus destinations controlled by malicious actors (otherwise known as DNS spoofing). This means that malicious actors can intercept traffic from unsuspecting users, and misdirect them to malicious domains for data theft or financial gain.

The Domain Name System Security Extension (DNSSEC) protocol was developed to provide a layer of security to the DNS. The DNSSEC ensures that the website that the user is accessing corresponds with the correct domain name, which prevents malicious actors from redirecting users to a fake website or service.

CSA is working with the IMDA and the Internet Service Providers to implement DNSSEC across Government agencies and local Internet domains to protect users from the inherent DNS vulnerabilities. This is one way where we are augmenting the security of the Internet to prevent these threats from ever reaching Internet users.



2 Strengthen cybersecurity of Cloud services

Protecting our Cloud frontier

What is the need?

Cloud computing has become the de facto platform catalysing and supporting the delivery of digital services and the storage of data. The Government supports the development of a robust Cloud ecosystem and the adoption of Cloud services across our industries and economy, as it raises Singapore's overall competitiveness in the digital domain toward our Digital Economy objectives. However, with greater reliance on and adoption of Cloud services comes the need to strengthen Cloud cybersecurity, so that services and data hosted on the Cloud are better protected against malicious actors looking to exfiltrate sensitive data or disrupt a company's services.

What will we put in place?

The IMDA, together with CSA, is working with Cloud service providers, industry certification bodies, industry associations, professional bodies, academia and SME representatives to review and update the Multi-Tier Cloud Security (MTCS) standard to mitigate the latest security concerns in Cloud Native environments.

The MTCS standard was first developed in 2013 by then-Infocomm Development Authority and the industry to provide enterprises in Singapore with greater clarity on the levels of security offered by the different Cloud service providers, and encourage the adoption of Cloud security risk management practices in our enterprises. It takes a risk-based approach to the security controls adopted by Cloud service providers, depending on the business impact of the subscribed services that enterprises rely on. There are three tiers of security controls that commensurate with the criticality of the enterprise's data and systems. For instance, for non-critical business data and systems hosted on the Cloud, the MTCS standard proposes baseline security controls. For enterprises that own high-impact, critical information systems on the Cloud, more stringent security controls are adopted that commensurate with the cybersecurity risks faced.

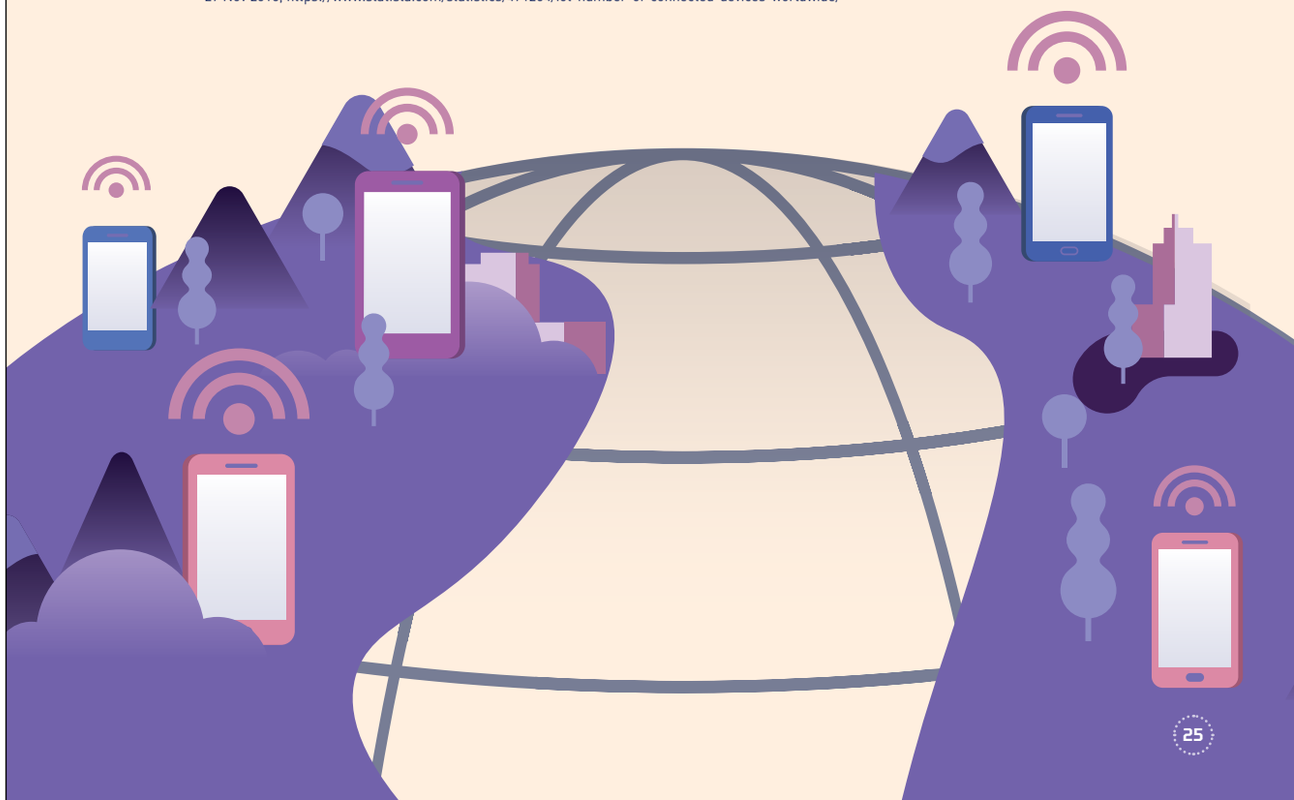
Together with the Cloud consumers and industry certification bodies, the updated MTCS standard, which will be published in late-2020, is envisaged to raise the cybersecurity posture of Cloud services in Singapore, and provide our enterprises and users with the peace of mind that their data and systems hosted on the Cloud are adequately protected.

Securing User Devices and Endpoints

Besides protecting the Internet infrastructure, we also need to secure our end-user devices and endpoints, where vulnerabilities are also commonly found. Developers and manufacturers, besides users, should also take responsibility for the security of connected devices and endpoints, as they are better placed to address vulnerabilities in such devices.

The Internet of Things (IoT) is expanding at a staggering rate. The number of IoT devices globally is expected to increase five-fold between 2015 and 2025, reaching more than 75 billion devices by 2025.[13] That amounts to more than nine IoT devices on average for every person in the world. With the widespread use of IoT devices and hence increased likelihood of malicious cyber activities arising from such devices, we must ensure that they are designed and manufactured with cybersecurity in mind, and with adequate cybersecurity measures put in place.

[13] Statista Research Department. "Internet of Things — number of connected devices worldwide 2015-25", 27 Nov 2016, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/



3 Offer cybersecurity labelling regime for IoT devices

Let's be cyber smart about smart devices

What is the need?

IoT devices are devices we use that are connected to the Internet. Our CCTV cameras, baby cameras, Smart TVs and Smart Home hubs are all IoT devices. Many of such devices do not come with robust cybersecurity measures, because product developers are today not required to put in security measures that protect the user. Manufacturers are often under pressure to place their products on the market as soon as possible at the lowest price. Both factors result in less-than-adequate cybersecurity measures, since the need to implement security would likely raise the cost and increase the time to market. This is not ideal.

Consumers and users of IoT devices face significant risk when using products with weak security — for example, CCTV cameras can be hacked to access the video footage, and Smart Home hubs can be compromised to gain the user's personal data. There is a strong need to implement better cybersecurity controls in these devices, to safeguard the safety and privacy of our users.

Is your connected device compromised?

From connected cameras to smart lights, IoT devices have brought many conveniences to our lives. However, many IoT devices are not set-up with proper security configurations.

For example, malicious actors can exploit default security configurations to hijack IoT devices. In 2016, the Mirai botnet took advantage of 61 default password combinations to create an army of an estimated 100,000 infected devices (or botnet drones) in 164 countries, ranging from printers, thermostats, Wi-Fi enabled clocks to baby monitors. The Mirai botnet attacked Internet servers to deny users access to popular websites including Twitter, Netflix and Airbnb for almost 12 hours.

Cybersecurity Labelling Scheme

BY CYBER SECURITY AGENCY OF SINGAPORE

What will we put in place?

The Government will offer a Cybersecurity Labelling Scheme (CLS) that device manufacturers can voluntarily apply for, which provides different levels of cybersecurity ratings to help consumers easily assess the level of security offered by a smart device and make informed choices. These labels indicate the security provisions of the registered products, based on a series of assessments on:

- **Meeting basic security requirements such as ensuring no universal default password;**
- **Adherence to the principles of Security-By-Design;**
- **Absence of common software vulnerabilities; and**
- **Resistance to common cyber-attacks.**

In this way, consumers can be more discerning and choose to buy more secure products. With increased consumer demand for security, manufacturers and developers will also be incentivised and encouraged to develop products with recognised and improved security features.

As a start, CSA will introduce the CLS to a few product types, such as home Wi-Fi routers and Smart Home hubs. These products are prioritised because of the impact that a compromise of such products could have on users. Home Wi-Fi routers are critical network devices that provide us with access to the Internet and process network traffic within our homes, while Smart Home hubs control the functioning of the Internet-connected devices in our homes. In particular, for home Wi-Fi routers, IMDA will also set minimum security requirements as part of the interoperability and communication standards. IMDA has also published an IoT Cyber Security Guide to offer enterprise users and their vendors better guidance on deploying IoT systems and technology.

Moving forward, CSA will work with like-minded international partners to establish mutual recognition arrangements for the CLS, as Singapore is a small market with limited ability on our own to shift the global IoT device market toward an enhanced security standard. This will involve aligning the CLS with widely accepted global security standards for consumer IoT devices.

Safeguarding Enterprise Applications

4 Leverage the National Digital Identity trusted services, such as MyInfo and SingPass Login, for identity assurance and authentication

What is the need?

The final tier of our digital infrastructure involves applications. Security vulnerabilities also arise at the application level, such as those on our laptops, mobile devices and Internet platforms like e-commerce and payment websites.

These vulnerabilities put users at risk when they access these applications and reveal their personal and financial data, which may then be exploited by malicious actors or cybercriminals, as many applications have weak identity assurance and authentication assurance processes. For example, a cybercriminal could create fake accounts within the e-platform to scam victims, which may be prevented if identities of users on such platforms are robustly verified. Malicious actors could also leverage gaps in authentication to access victims' accounts for financial gain. We aim to encourage the adoption of best practices to address such vulnerabilities as far as possible.

One login to rule them all: identity assurance and authentication with National Digital Identity trusted services

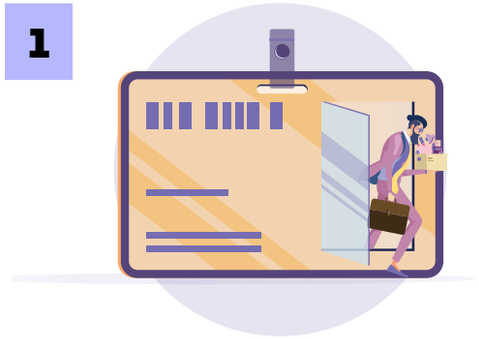
What have we put in place?

The Government will continue to enhance the cybersecurity of our Information and Communications Technology (ICT) and smart systems. These applications and tools, including the National Digital Identity (NDI)'s trusted services of MyInfo and SingPass Login, are made secure-by-design to support enterprises and individuals when transacting with Government agencies.

Besides using these NDI services for transactions with the Government, enterprises are also encouraged to leverage them to augment their own identity assurance and authentication processes. Enterprises would be able to verify the identity of users on their platform at the point of user registration and confirm that they are indeed who they claim to be, which constitutes electronically 'knowing your customer'. In addition, enterprises can authenticate users logging into their e-platform using these trusted services, either as an alternative to the enterprise's own authentication systems or as enhanced authentication for more sensitive transactions. This applies for sectors including banking and finance, telecommunications, tourism, e-commerce and many others.

The benefits for enterprises to use NDI trusted services are two-fold:

1



First, it raises the security posture of the e-platforms used by enterprises. For example, if all local users on e-platforms logged in via SingPass, users would have significantly higher assurance of the authenticated identity of the parties they were transacting with. This protects users by reducing the likelihood of malicious actors claiming to be who they are not on these e-platforms.

2

Second, enterprises can augment their own identity verification processes using MyInfo and SingPass for added assurance. With this, users would not need to go through lengthy 'know your customer' processes to register with the enterprise, which enhances convenience for the user.

Enterprises must apply and be approved by the Government before using NDI Application Programming Interfaces (APIs). To protect the security of the data maintained by the Government, enterprises are not permitted to request for more data than is required for their purposes, and will need to justify the request for confidential data with explicit approval granted by the user. Enterprises interested to sign up to leverage NDI trusted services can get started at the NDI API Portal at https://www.ndi-api.gov.sg/.

CHAPTER 3

Safeguarding Our Cyberspace Activities

The second strategic thrust of the Safer Cyberspace Masterplan entails the **swift detection of malicious cyber activities via the national-level detection and analysis of cyber threats, and the protection of enterprises against potential malicious cyber activities through self-help tools and solutions.**

As cyber threats exploit the vulnerabilities in our Internet architecture, user devices and endpoints, and applications — despite the measures detailed in Chapter 2 — we must ensure that these threats are quickly detected and remediated. The measures outlined in this chapter help to ensure that **the impact and damage caused by cyber threats is kept to a minimum**. The next Chapter — Chapter 4 — will articulate how our population will be empowered through cyber awareness and adoption to support our objective of a safer and more secure cyberspace in Singapore.

National Detection and Analysis of Malicious Cyber Activities

The Government will strengthen Singapore's national malicious cyber activity detection and analysis capabilities, as follows:

5 Leverage human-Artificial Intelligence collaboration for swift detection and response to malicious cyber activities

What is the need?

Addressing vulnerabilities and implementing security-by-design measures in our Internet architecture, user devices and endpoints, and applications, is not a fool-proof strategy. These efforts mitigate the cyber risks we face, but we must also be prepared for the inevitability of a threat breaking through our defences. We need to develop the ability to swiftly detect and respond to these threats.

Our robo-hound that sniffs out sneaky cyber rodents

What will we put in place?

CSA will implement a Cyber Fusion Platform capable of assimilating and analysing information from a myriad of sources. This will allow CSA to swiftly triage high-priority cyber evidence that may be warnings of impending malicious cyber activities, correlate evidence across all cybersecurity information sources, and conduct the requisite investigations with enhanced efficiency. This automation of threat detection and analysis, coupled with human knowledge and expertise in cybersecurity, will allow Singapore to develop a national early warning system against malicious cyber activities.

A key feature of the Cyber Fusion Platform is the use of Artificial Intelligence (AI) engines in cybersecurity. AI will play a key role in transforming cybersecurity, and the cybersecurity domain is one of nine key sectors identified under the National AI Strategy launched by the Smart Nation and Digital Government Group (SNDGG) in November 2019. The Cyber Fusion Platform demonstrates how the Government is accelerating the build-up of domestic capabilities in AI cyber analytics to meet Singapore's strategic needs. The AI-powered analytic engine will be able to:

- **Perform automated predictive trend analysis.**
- **Auto-correlate cyber evidence from all information feeds and achieve early warnings of malicious cyber activities.**
- **Reduce dependence on cyber analysts to deal with voluminous data and hasten the speed at which cyber threats can be detected and responded to.**

These AI functions will augment the expertise and capabilities of our cyber analysts, and enable the swift and effective detection of threats in our cyberspace, thereby minimising the impact and damage to Singapore and Singaporeans.

Feature: Artificial Intelligence

National AI Strategy and how AI can transform cybersecurity

National AI Strategy

The National AI Strategy is a key step in Singapore's Smart Nation journey. It was launched in November 2019 with the vision of putting Singapore at the forefront in the development and deployment of scalable and impactful AI solutions in sectors of high value and relevance to our citizens and businesses.

The National AI Strategy is driven by two main components: the deployment of National AI Projects with high social and/or economic impact, and the strengthening of AI ecosystem enablers. The Strategy identifies nine key sectors to focus attention and resources at a national level. These key sectors are Transport & Logistics, Manufacturing, Finance, Safety & Security, Cybersecurity, Smart Cities & Estates, Healthcare, Education and Government. The deployment of AI in these sectors serves to realise significant social and economic good for Singapore — for instance, the early detection and management of chronic diseases.

The Strategy also sets out how the Government, companies, and researchers can work together to realise positive impact from AI. Talent, data, regulation, and effective deployment are key elements in enabling AI applications that serve society. The Strategy further addresses areas where attention is needed to manage change and/or manage new forms of risks that arise when AI becomes more pervasive. These include workforce adaptation and the governance of decision making by machines.

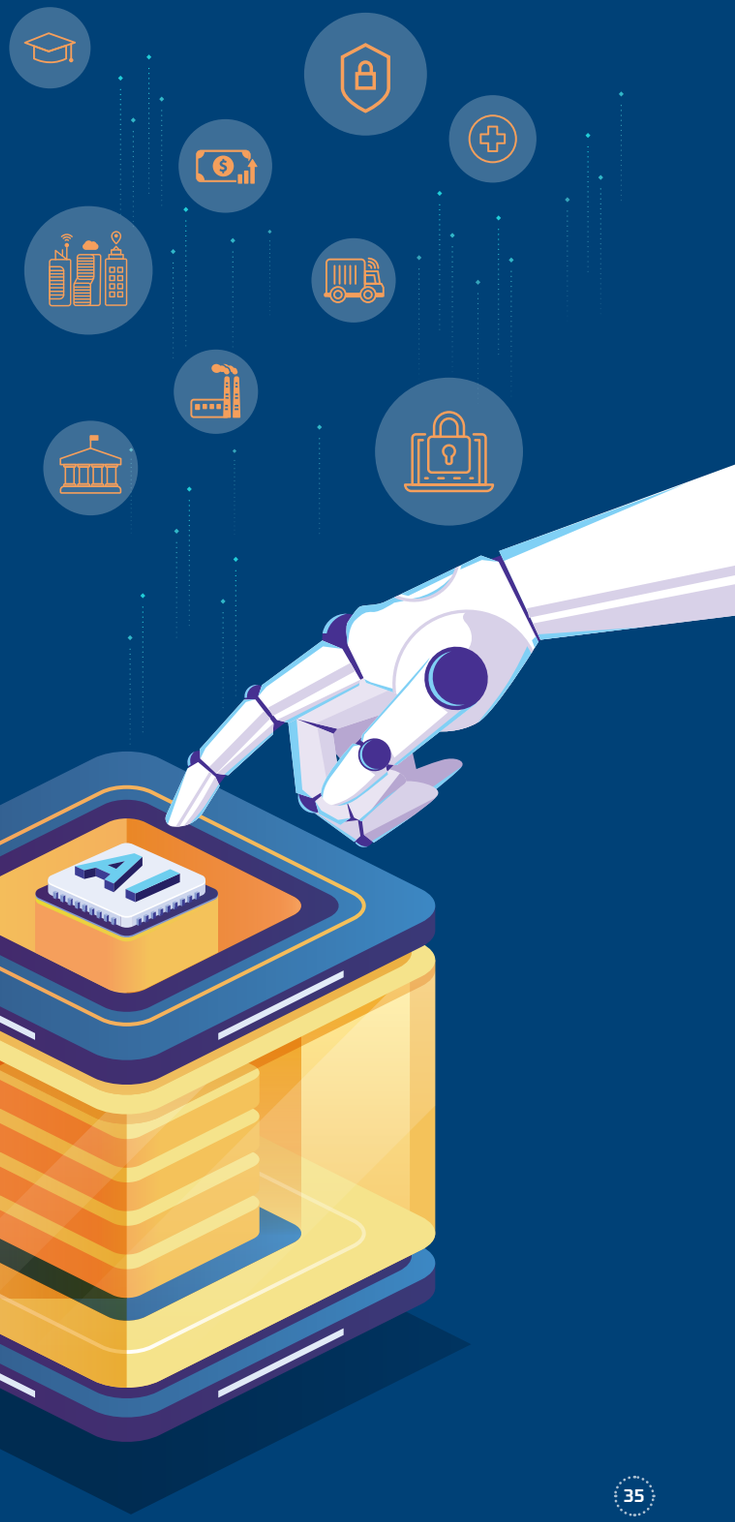
The National AI Strategy sets out a cohesive plan in making Singapore a leading country in AI, and more broadly a Smart Nation for our citizens.

Scan to find out more details about the National AI Strategy.

AI in Cybersecurity

AI is one of the key emerging technologies that will shape the cybersecurity landscape in the near future. While AI can significantly enhance the capabilities of cybersecurity systems, such as AI-enabled automated anomaly detection and threat response, there are challenges too. As the use of AI in cybersecurity systems increasingly becomes mainstream, there are concerns that AI systems can be 'poisoned' with malicious data to misdirect AI systems into making wrong and costly decisions.

To stay ahead of the rapidly evolving threats, CSA has funded research initiatives to look into AI in cybersecurity, through the National Research Foundation's National Cybersecurity R&D programme and CSA's Cybersecurity Industry Call for Innovation. One example is the formulation of guidelines in developing, training and honing robust AI engines for cybersecurity purposes.



6 Allow early detection and response to impending IoT attacks by monitoring global developments in IoT threats and vulnerabilities

What is the need?

One area of specific concern is threats to our IoT devices — as earlier described, we expect the global number of IoT devices to rise to more than 75 billion by 2025. This presents a huge attack surface for malicious actors, which may lead to consequences like the theft of our personal data and the disruption of services using IoT devices as botnet drones to conduct Distributed Denial of Service (DDoS) attacks. We need advanced monitoring mechanisms to help us keep up with the rapidly evolving global IoT threat and vulnerabilities landscape.

What will we put in place?

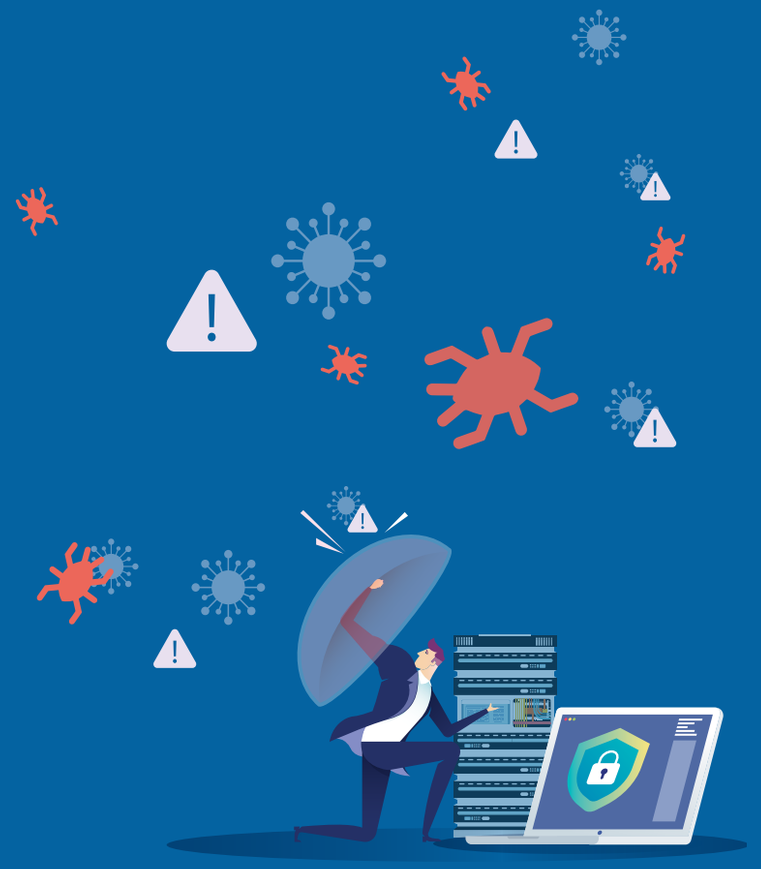
There is a need to proactively watch for global IoT threats and attack data, so that Singapore can be better prepared before the next wave of botnet attacks hits our shores and results in non-functional devices — and worse yet, devices that serve as botnet drones conducting malicious cyber activities on us.

CSA will be working with our partners to set up an IoT Threat Analytics Platform. This will provide CSA with information on, and analysis of, the global IoT threat landscape. Through this analysis, CSA can better detect impending, large-scale IoT attacks and assess the impact before they happen. These insights from the IoT Threat Analytics Platform will allow CSA and other Government agencies to put in place policy and technical measures to safeguard the cybersecurity of IoT devices and address the threats before they cause damage. Coupled with the Cybersecurity Labelling Scheme detailed in Chapter 2, these initiatives improve cybersecurity in the IoT space in order to allow Singaporeans to enjoy the conveniences and opportunities these devices bring.

Understanding the global IoT threat landscape

Enabling Enterprises to Protect Themselves from Cyber Threats

It is essential that enterprises and organisations play their part to take ownership and responsibility for their online security. The Government will enhance its role by making cybersecurity resources available for enterprises and organisations. These self-help tools and solutions will help safeguard our digital activities against threat actors, and mitigate the impact of malicious activities.



7 Create an Internet Cyber Hygiene Portal for users to self-assess their domain, email and connectivity health, and address identified vulnerabilities

What is the need?

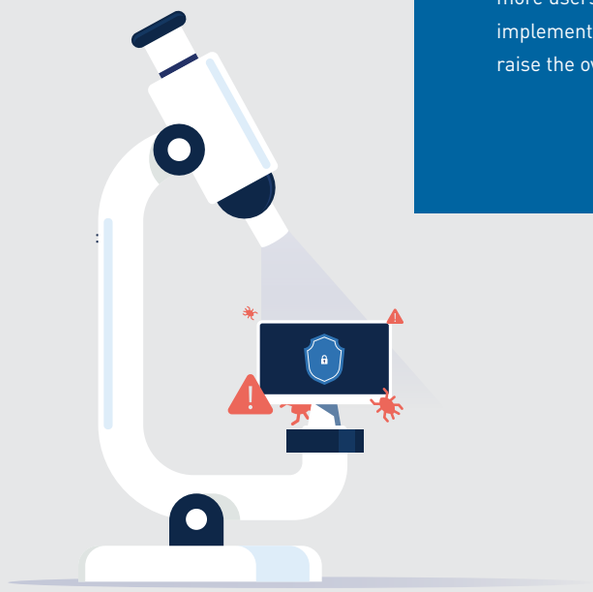
Many enterprise users do not know the cyber health of their own domains, email systems and connectivity to the Internet. They may also not know where to go to seek assistance on whether they are sufficiently cyber secure, and what they can do if they are not. The gap faced today is the lack of an easily-accessible, trusted avenue for enterprise users to self-check if their cyber defences are robust — and where they are lacking, provide advice on cybersecurity measures they should put in place.

Health screenings for your websites and domains

What will we put in place?

CSA will be developing an Internet Cyber Hygiene Portal. The benefits of the Portal are two-fold: first, the Portal will provide cyber guides and toolkits housed in a single location at CSA's webpage, making it easier for users to access self-help resources and adopt cyber best practices; second, the Portal incorporates cyber health lookup tools that help enterprise users to assess their domain, email and connectivity cyber health.

These are critical cyber health indicators, and their cybersecurity status will be reported to the enterprise user along with actionable suggestions on how users can improve their cybersecurity. This includes encouraging the adoption of Internet best practices, such as the DNSSEC protocol and email hygiene practices. In this way, enterprise users can readily access resources on Internet security best practices and standards, and receive advice to improve their own cybersecurity. This one-stop Portal also simplifies cybersecurity for the user to only key indicators that matter. Over time, as more users leverage the Portal to assess their cyber health and implement measures to augment their cybersecurity, this will raise the overall cybersecurity posture for Singapore.



8 Design easy-to-use cyber solutions for enterprises

Your one-stop cybersecurity solution

What is the need?

Almost every cyber-attack involves the use of software. One effective strategy to deal with such malicious cyber activities is to disallow software from working, unless explicitly verified as trusted software. This creates a 'zero-trust' cyber environment to enhance our cybersecurity posture against malicious applications and software. The seven essential cybersecurity principles (i.e. the 'Cybersecurity Essentials') to implement this 'zero-trust' environment are as follows:

Know your Assets

Give the Right Admin 'Passes'

Timely Patching and Updating

Allow only Authorised Software to Work

Detect Breaches Promptly

Access Control

Encrypt your Crown Jewels

However, users may not know how to implement these 'Cybersecurity Essentials', especially SMEs who may lack the expertise or resources to determine the most cost-effective cyber solutions to put in place to safeguard themselves in cyberspace.

What will we put in place?

CSA is collaborating with local cybersecurity industry partners to design an architecture for an integrated and automated Security-as-a-Service (SaaS) solution that incorporates all the 'Cybersecurity Essentials', to better protect enterprise users from malicious cyber activities.

The objectives of this are three-fold:

Secure computers and achieve swift detection and response to malicious cyber activities;

Reduce the demand for cybersecurity manpower, which is a scarce resource, through the automation of cybersecurity services; and

Define the standards for interoperability for the SaaS components to overcome the challenges that users face in integrating several different cyber solutions. Vendors who wish to integrate their tools into this may do so.

At the core of this solution is the ability to allow only trusted applications and software to be executed by the Operating System. This is in essence application control, such that malicious, untrusted applications and software cannot be executed — and hence cannot cause damage to users. In addition, the solution will protect data through encryption, thereby preventing data exfiltration in unencrypted (i.e. easily-readable and accessible) form.

This SaaS solution will be able to defend against threats including malware sent via phishing emails, ransomware, hijacked privileged administrator accounts and insider threats, among others. The implementation of this solution will simplify cybersecurity for the users, raise their cybersecurity posture, and better protect users from the myriad of evolving cyber threats. The SaaS solution will be made available for SMEs under Enterprise Singapore's Productivity Solutions Grant[14] and IMDA's SMEs Go Digital programme.

[14] Eligible SMEs can receive funding support under the Productivity Solutions Grant (PSG) of up to 80% (enhanced from 70% to 80% till 31st December 2020) of the qualifying cost (e.g. subscription, license, and installation fees) of preapproved cybersecurity products and services for 12 months. Besides funding support, enterprises are provided with an interactive self-assessment checklist of 13 critical cybersecurity measures, that serves to enhance awareness of the best practices and processes they should implement and suggest suitable pre-approved cybersecurity solutions they could adopt based on their current cybersecurity posture.

CHAPTER 4

Empowering Our Cyber-Savvy Population

The third and final strategic thrust of the Safer Cyberspace Masterplan looks at empowering our cyber-savvy population to deal with cyber threats, through **enhanced awareness of how to protect ourselves in cyberspace, changing attitudes toward cybersecurity and the adoption of appropriate measures.** These contribute toward strengthening cyber resilience among enterprises and individuals, through better protection, response and recovery against cyber threats.

It is often cited that people are the weakest link in any cyber defence. It is therefore imperative for users to be cognisant of the cybersecurity risks they face, the potential consequences of such risks, and how they can be better protected against them. Through CSA's engagement with the private sector, cybersecurity industry and members of public, we have identified three key problems:

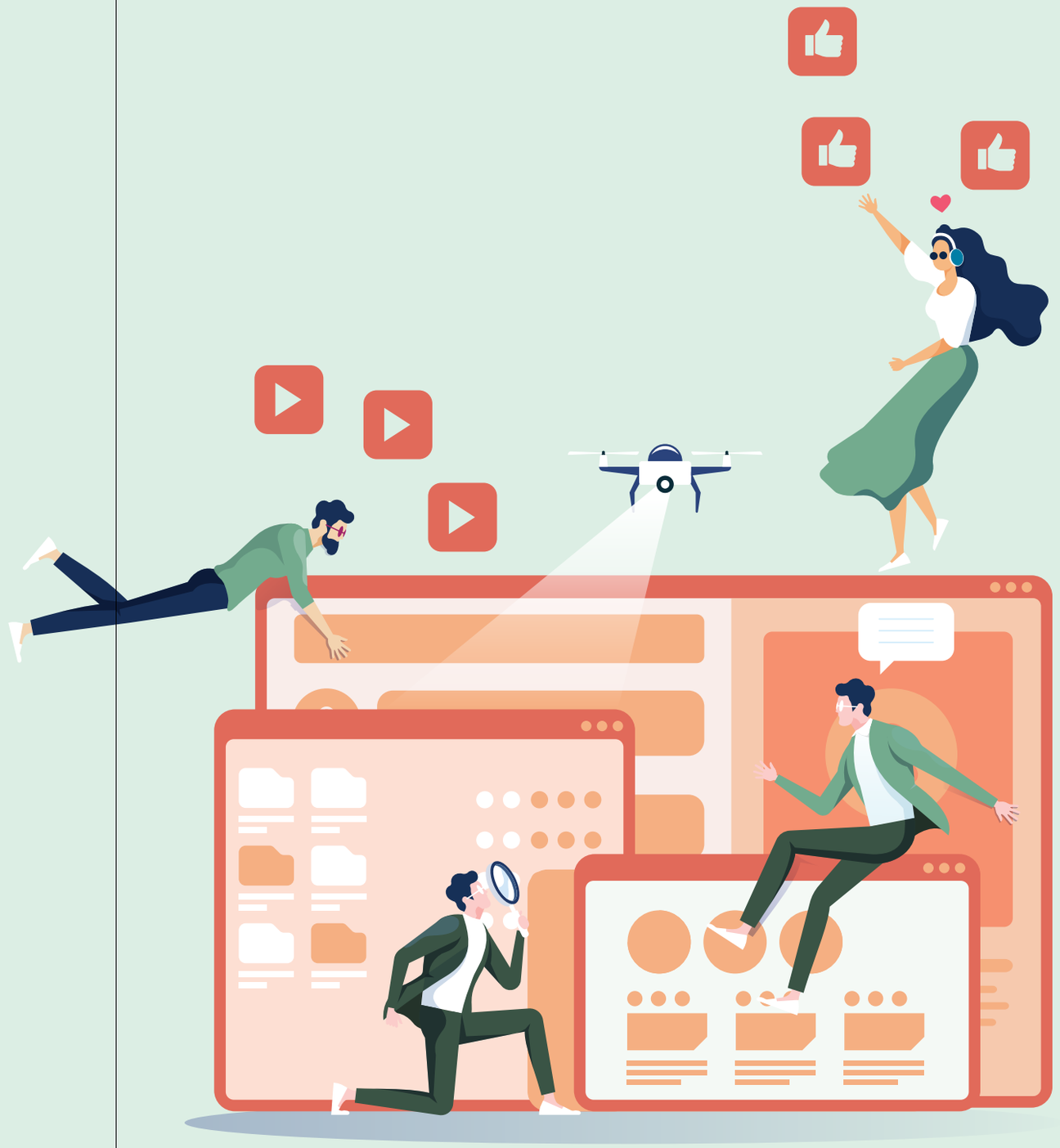
• **Lack of awareness: More than 4 in 10 Singaporeans** are unable to correctly identify strong passwords, and **only 4% of survey respondents** could correctly identify phishing emails from legitimate ones.

• **Lax attitudes**: **About 4 in 5 Singaporeans** are moderately or extremely concerned about malicious cyber activities (such as computers being controlled by hackers illegally or personal information being obtained by others without consent).[15] But **less than 2 in 5 Singaporeans** feel that such malicious cyber activities would happen to them.

• **Low adoption: Close to 3 in 5 Singaporeans** do not enable Two-Factor Authentication for their social media or personal email accounts, although a large majority (close to 80%) did so for online banking services. This speaks to users being aware of the need for 2FA, but not adopting the practice.

For enterprises, **more than half of digital enterprises** in Singapore (i.e. enterprises that use computers and/or have Internet access) have no cybersecurity measures in place[16], while **close to 40% of all malicious cyber activities** in Singapore had targeted SMEs.[17]

These data-points speak to the need to step up cyber awareness efforts, change attitudes on cybersecurity, and go a step further to encourage the adoption of good cyber practices, toward cyber resilience within our population.



[15] Cyber Security Agency of Singapore. "CSA's Cybersecurity Public Awareness Survey shows that Singaporeans remain concerned about cyber incidents, but there is room for improvement in cyber hygiene", 21 Aug 2020, https://www.csa.gov.sg/news/press-releases/csa-public-awareness-survey-2019

[16] Infocomm Media Development Authority. "Annual Survey on Infocomm Usage by Enterprises for 2019", 2019, https://www.imda.gov.sg/-/media/Imda/Files/Industry-Development/Fact-and-Figures/Infocomm-Usage-Business/Infocomm-Usage-Survey-Public-Report-2019.pdf?la=en

[17] Cyber Security Agency of Singapore. "Cyber Threats in Singapore Grew in 2017, Mirroring Global Trends", 19 Jun 2018, https://www.csa.gov.sg/news/press-releases/cyber-threats-in-singapore-grew-in-2017-mirroring-global-trends

Raising Awareness and Changing Attitudes on Cybersecurity

The Government will augment existing cyber awareness programmes for enterprises and individuals, which also contribute toward shifting mindsets about the need to take precautions to avoid falling victim to cyber threats:

9 Raise enterprise awareness of cybersecurity through resources and toolkits

The first step to mitigating cyber threats: understanding cybersecurity

What is the need?

There are three tiers of needs for enterprise cybersecurity awareness today:

First, there is little formal guidance provided to the management teams of enterprises on what they should look out for when it comes to cybersecurity. Enterprise leaders, such as Board Directors and owners of SMEs, are key decision-makers on how cybersecurity risks are managed. Research conducted by McKinsey and the World Economic Forum[18] has indicated that management attention and time devoted to the issue is the single largest driver of better cybersecurity risk management. This outweighed other factors, including company size, sector that the company is in, and resources the company possessed. There needs to be **targeted guidance to enterprise leaders for them to make good decisions on addressing the cyber risks their enterprises face.**

Second, the majority of cybersecurity guidance provided to enterprises are catered for the Chief Information Security Officers (CISOs) and the cybersecurity teams they lead. This guidance is usually technical in nature, and **there is a gap to translate such technical guidance into easily understandable, actionable steps for the users they serve to raise their cybersecurity posture.**

Third, **employees also require guidance on how they can better protect themselves in cyberspace and how to respond when they experience a malicious cyber activity.** This cannot only be the responsibility of the enterprise cybersecurity team or the CISO, but instead **a collective responsibility.** As frontline users of computer systems, employees can be the first and most effective line of defence, or the weakest link. It is in the enterprise's interest to ensure the former instead of the latter.

[18] Bailey, Tucker, Kaplan, James and Rezek, Chris. "Why senior leaders are the front line against cyberattacks", 1 June 2014, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks

What will we put in place?

CSA will develop and promulgate targeted resources and toolkits for each of these three categories of stakeholders, according to their different knowledge needs and role in the enterprise.

Enterprise leaders

Enterprise leaders are **key decision-makers** for the enterprise's cybersecurity strategy and resource allocation. The guidance will take the form of practical toolkits that translate cybersecurity for the non-technical leaders, on how to better manage and oversee their enterprises' cyber risks.

Employees

Employees are **frontline users** and the first line of defence. The guidance will show them how they can play a part in their enterprise's cyber defence and protect their enterprise's assets. As a start, CSA will work with the Smart Nation and Digital Government Group to tailor cybersecurity modules intended for public officers for employees in the private sector.

CISOs and cybersecurity teams

CISOs and cybersecurity teams are **implementers** of the enterprise's cybersecurity strategy. The toolkit for this group of stakeholders will not only focus on the technical aspects of cybersecurity, but also include how they can better drive the enterprise's desired cybersecurity outcomes and translate cybersecurity for their non-technical stakeholders, such as their management team and employees of the enterprise.

One example is the Exercise-in-a-Box Singapore (EiaBSG) tool that CSA will be launching in partnership with the United Kingdom's National Cyber Security Centre. Designed to complement organisations' existing cybersecurity measures, the EiaBSG tool will provide organisations in Singapore with a safe environment to exercise and test their response to a variety of cyber-attack scenarios. Organisations can use the tool to assess their cyber resilience and readiness, identify possible gaps in their cybersecurity, and better prepare against such cyber-attack scenarios.

Over the years, CSA has put in place the following initiatives to engage enterprises and raise their cybersecurity awareness:

- The Singapore Computer Emergency Response Team (SingCERT) promulgates cybersecurity advisories (QR code to the URL on the left) to businesses and the public on new threats and vulnerabilities as they arise, and provides recommendations on how businesses and members of the public can pre-empt and prevent malicious cyber activities from happening to them.
- CSA issues publications, such as the Be Safe Online handbook (QR code to the handbook on the left), that identifies key cybersecurity measures that enterprises should adopt to protect their data and assets.
- CSA also monitors cybersecurity trends and publishes an annual Singapore Cyber Landscape report (QR code to the latest 2019 report on the left) that reviews Singapore's cybersecurity situation against the backdrop of global cyber trends and threats, and highlights Singapore's efforts in creating a safe and trustworthy cyberspace.
- CSA also supports enterprise cybersecurity awareness in partnership with various stakeholders. For example, CSA partnered with the Association of Information Security Professionals (AiSP) to organise the SME Conference for Cybersecurity Awareness 2019 to engage our SMEs on good cybersecurity practices.

10 Raise community and individual awareness of cybersecurity by customising and implementing outreach approaches for different demographic segments

Inculcating good cyber hygiene practices has no age limit

What is the need?

There is a need to take a **community-centric approach** to cybersecurity. Beyond raising awareness among individuals, a community-centric approach involves encouraging cyber-savvy members of the community to spread their knowledge about what we can do to protect ourselves online to their family members, peers and social circle. In this way, individuals can act as community champions of cybersecurity and cyber hygiene, and contribute toward equipping more Singaporeans in their community with the cybersecurity know-how. To this end, CSA strives to cultivate good cyber hygiene practices from a young age among our students and youths, and also reach out to our seniors to ensure that they are kept cyber-safe. We will continue to leverage the strength of our community to spread the word about cybersecurity.

Feature: Tackling Online Harms

The Triad of Enhancing Cybersecurity, Mitigating Cybercrime and Protecting Personal Data

Cybersecurity is inherently related to cybercrime and personal data protection. Raising the national cybersecurity posture in Singapore would help to mitigate cybercrime and strengthen online personal data protection too. To create a safer cyberspace in Singapore, we need to tackle the adjacent online harms of cyber threats, cybercrime and data breaches comprehensively.

To this end, CSA partners with the Singapore Police Force (SPF), the National Crime Prevention Council (NCPC) and the Personal Data Protection Commission (PDPC) to raise awareness of these online harms, and provide actionable steps and advice for members of the public to better protect themselves in cyberspace. CSA has collaborated with PDPC and SPF to produce a series of Cyber Safety Activity Books to raise awareness of the importance of cybersecurity and personal data protection, as well as provide young readers with information on how to navigate cyberspace safely and spot online scams. CSA also collaborates with SPF and NCPC to feature cybercrime cases, such as Singapore's first Dark Web-related conviction on Mediacorp's longest-running info-educational programme Crimewatch. CSA participates actively in NCPC's Anti-Scam roadshows to spread cybersecurity messages and know-how to members of the public.

These joint efforts underscore the recognition that online harms are multi-faceted, and require multi-stakeholder collaboration for effective mitigation. This is especially important given the push toward digitalisation in the Covid-19 environment, so that members of the public can continue to stay safe and secure as our day-to-day activities increasingly shift online.

CSA's Cybersecurity Awareness posters from the 2019 National Cybersecurity Awareness Campaign, which were deployed in various public locations to raise awareness of good cyber hygiene practices

What have we put in place?

CSA's GoSafeOnline Community Outreach Programme provides bite-sized and actionable advice to keep everyone secure in the digital domain:

1 **General public:** CSA has been organising an annual National Cybersecurity Awareness Campaign since 2017. The campaign has been a mainstay of our cybersecurity awareness efforts, expanding its reach through the years with roadshows and creative ad campaigns.

To better highlight the cybersecurity messages, CSA introduced a Password Café at our roadshows in 2018 and 2019, where participants tried their hands at creating a strong password in exchange for drinks and snacks. Interactive games were also introduced to enable members of the public to learn cybersecurity tips in a fun way.

Four Cyber Tips:

The campaign encourages the adoption of four key cyber tips to stay secure online.

- **Use strong passwords and enable Two-Factor authentication**
- **Use an anti-virus software**
- **Update software as soon as possible**
- **Spot signs of phishing**

To learn more about these tips, scan this QR code.

A volunteer Cyber Champion explains to roadshow visitors how they can spot signs of phishing at the 2019 roadshow at Our Tampines Hub

Seniors learning how to go online securely, supported by IMDA's Digital Ambassadors

An officer from the Technology Crime Policy Branch of the Criminal Investigation Department, SPF, shares with a member of the public how to prevent oneself from falling victim to online scams at the Digital Inclusion Festival 2019

2 **Working adults and seniors:** To reach out to working adults and seniors, CSA works with our partners to give talks at various platforms such as conferences and community centres, and provide training resources for SkillsFuture courses. Cybersecurity resources for seniors are also made available on IMDA's Seniors Go Digital website and shared at the SG Digital Office community hubs, where seniors receive one-to-one assistance to pick up digital skills.

In June 2020, CSA supported IMDA's SG Digital Office in training about 1,000 Digital Ambassadors as part of their outreach efforts to engage seniors and stallholders to go digital. The Digital Ambassadors were trained on the common cybersecurity threats today, tips for using e-payment solutions securely, and cyber hygiene practices to stay safe online. These Ambassadors will integrate cybersecurity tips and awareness as they engage seniors and stallholders on their digitalisation journey.

A representative of RSA Security, a member of the Cyber Security Awareness Alliance[19], gives a talk on cybersecurity to Guang Yang Primary School students in Oct 2019

3 **Students:** Cybersecurity outreach is also conducted through the schools to our youths and students. Cybersecurity content has been incorporated in schools through collaborations with IMDA and the Ministry of Education (MOE).

Students learn how to use digital technologies safely and responsibly in Cyber Wellness lessons, through discussions on authentic case scenarios and reflection. Cybersecurity talks are also conducted for schools and Institutes of Higher Learning. CSA will work with IMDA and MOE to include cybersecurity activities in the Code for Fun programme for upper primary school students. In this way, students learn about cybersecurity at the same time as they develop computational thinking and coding skills.

[19] The Cyber Security Awareness Alliance aims to create a positive cybersecurity culture in Singapore, and promotes and enhances awareness and adoption of essential cybersecurity practices for both the private and public sectors. It comprises members from the Government, private enterprises, trade associations and non-profit organisations. The Alliance is co-led by CSA and SGTech, which is a trade association for the local tech industry.

Feature: Outreach to Students

CSA has developed resources and interactive modalities over the years to emphasise the importance of cybersecurity to students and youths. Examples include:

Cyber Safety Activity Books. From 2016 to 2019, CSA, in collaboration with the Personal Data Protection Commission, has produced five issues of the Cyber Safety Activity Book to raise awareness of the importance of cybersecurity and personal data protection. In 2020, CSA collaborated with the Singapore Police Force (SPF) to develop "Cyber Safety: The Interactive Handbook" to help readers navigate cyberspace safely, including ways to spot online scams. Close to 250,000 issues of the Cyber Safety Activity Book series and handbook have been distributed to Primary 5 students in Singapore.

"Go Safe Online" Drama Skit, which was staged at secondary schools to encourage students to adopt basic cyber hygiene practices essential to stay safe online. This is part of CSA's ongoing efforts to make our cybersecurity messages memorable for easy retention by our target audience. The Drama Skit pilot run concluded in December 2019, reaching out to close to 40,000 students.

Cyber Savvy Machine Pop-Up, which was launched in 2018. The Pop-Up, consisting of an interactive vending machine and information panels, showcases cybersecurity tips and a quiz for the public to test their knowledge. It has travelled to libraries, Community Clubs and schools over 16 months and ended its tour in February 2020. More than 100,000 quiz attempts were recorded.

Enhancing Cyber Adoption

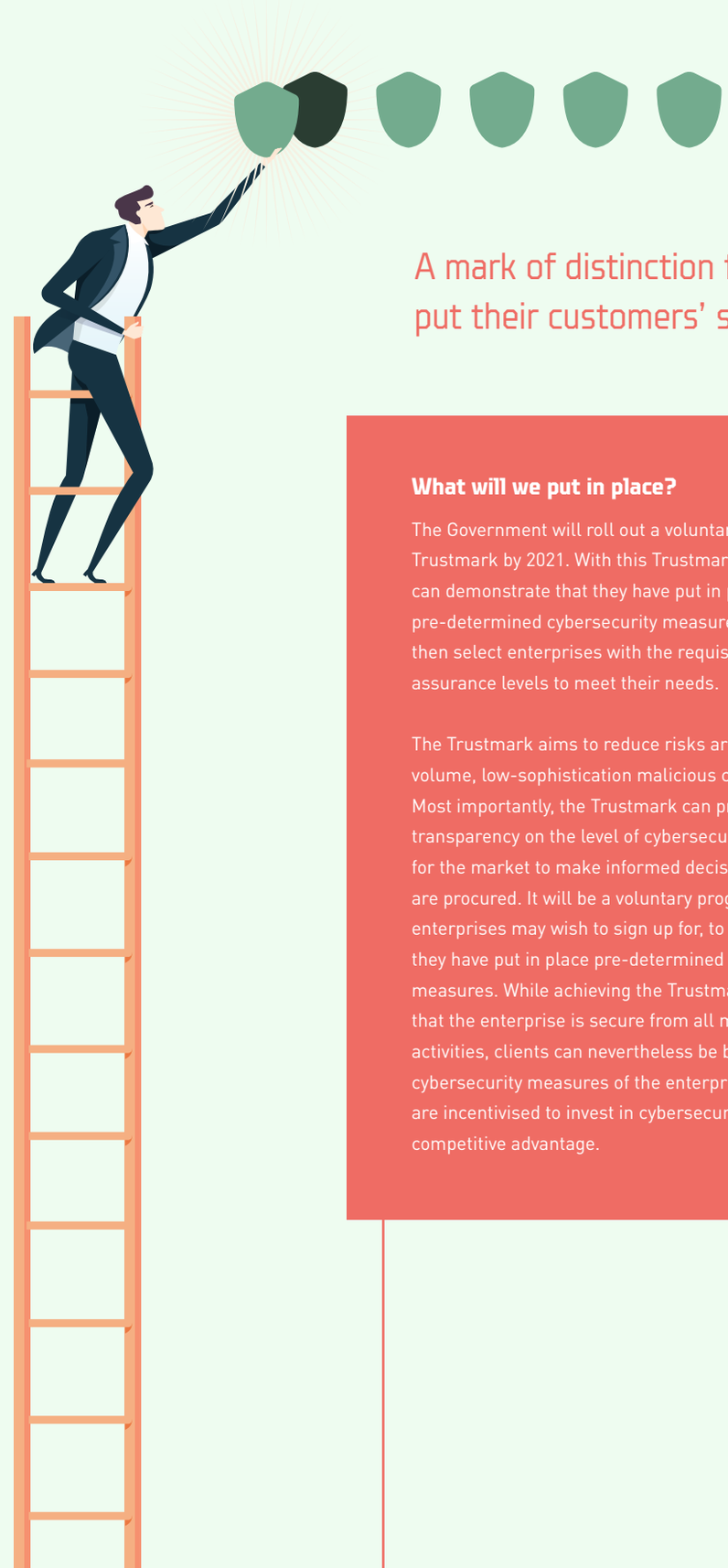
It is not sufficient just to be aware of cyber threats. Cyber awareness needs to be translated to adoption of good cyber hygiene practices, as follows:

11 Enhance enterprise adoption of cybersecurity through a new SG Cyber Safe Trustmark

What is the need?

Cybersecurity continues to be viewed as a business cost that detracts from the enterprise bottom-line, with no clear return on investment. Therefore, enterprises understandably do not have a strong incentive to put in place good enterprise cybersecurity practices.

We need to shift the thinking of cybersecurity as a cost, to cybersecurity as a competitive advantage for the enterprise. There is a need to help identify and profile enterprises that meet pre-determined cybersecurity measures, so that they can be considered favourably in the market. In the long-run, this could incentivise all enterprises to invest more in cybersecurity.



A mark of distinction for those that put their customers' security first

What will we put in place?

The Government will roll out a voluntary SG Cyber Safe Trustmark by 2021. With this Trustmark, enterprises can demonstrate that they have put in place certain pre-determined cybersecurity measures. Clients can then select enterprises with the requisite cybersecurity assurance levels to meet their needs.

The Trustmark aims to reduce risks arising from high-volume, low-sophistication malicious cyber activities. Most importantly, the Trustmark can provide a degree of transparency on the level of cybersecurity of enterprises, for the market to make informed decisions when services are procured. It will be a voluntary programme that enterprises may wish to sign up for, to demonstrate that they have put in place pre-determined cybersecurity measures. While achieving the Trustmark does not mean that the enterprise is secure from all malicious cyber activities, clients can nevertheless be better assured of the cybersecurity measures of the enterprise, and enterprises are incentivised to invest in cybersecurity as it becomes a competitive advantage.

Conclusion

Toward a Safer and More Secure Cyberspace for Singapore and Singaporeans

The Safer Cyberspace Masterplan augments existing efforts to safeguard our Digital Economy and Smart Nation, and protect Singapore's cyberspace against cyber threats.

We want to work toward an inclusive, secure and thriving cyber ecosystem that undergirds digital opportunities and supports national digitalisation efforts. This is a cyberspace that Singaporeans from all walks of life must create and safeguard together to chart our collective digital future.

Glossary

Term	Definition
Two-Factor Authentication (2FA)	The approach to authentication using two authentication factors to reduce the probability that the requestor is presenting false evidence of its identity. The two authentication factors could be as follows: (1) Knowledge factor — "Something the user knows", such as a password, PIN and pattern; (2) Possession factor — "Something the user has", such as ATM card and security token; (3) Inherence factor — "Something the user is", such as finger print and retina scan.
Advanced Persistent Threat (APT)	An attack in which perpetrators successfully gain access to a targeted system and stay undetected for a long period of time to exfiltrate, modify, or destroy critical data. APTs can also refer to the advanced, and often state-linked or state-sponsored threat actors that conduct extended campaigns, such as cyber espionage.
Artificial Intelligence (AI)	Refers to the study and use of intelligent machines to mimic human action and thought.
Attack Surface	Referring to all vulnerable resources of a system, or the sum of the points through which an attacker could try to enter an environment.
Authentication Assurance	Authentication refers to the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system, based on the reliability of a set of credentials. Authentication assurance describes the degree of confidence that the user that presented the credential is in fact that user.
Botnets	An automated software program used to carry out specific tasks. A botnet is a network of compromised computers infected with malicious bots, controlled as a group without the owners' knowledge.
Cloud	A model for enabling ubiquitous, convenient, 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.
Command and Control (C&C) Servers	Centralised devices operated by attackers to maintain communications with compromised systems (known as botnets) within a targeted network.
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.
Data Breach	The unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data or confidential information in an organisation's possession or under its control.

Term	Definition
Distributed Denial- of-Service (DDoS)	Where an attacker attempts to prevent legitimate users from accessing information or services online. The most common and obvious type of DoS attack occurs when an attacker "floods" a network with information. In a distributed DoS attack, an attacker takes unauthorised control of multiple computers, which may be harnessed as a botnet, to launch a DoS attack.
Domain Name System (DNS)	Refers to the system used to translate readable domain names to Internet Protocol (IP) addresses.
Domain Name System (DNS) Spoofing	A type of cyber-attack that spoofs DNS records through methods including compromising a DNS server, mounting a DNS cache poisoning attack or mounting a man-in-the-middle attack.
Hacktivists	An individual or a group who wants to undermine the reputation or destabilise the operations of an entity, or to publicise their political or social agenda and gain recognition, usually by hacking an organisation's website.
Identity Assurance	Refers to the reliability of ID proofing process and the degree of confidence that the applicant's claimed identity is their real identity
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.
Malware	Malicious software intended to perform unauthorised processes that will have adverse impact on the security of a computer system, such as virus, worm, Trojan horse, spyware and adware.
Personal Data	Data which, on its own (e.g. full name, NRIC number) or in combination with other available data (e.g. medical or educational information), can be used to distinguish or trace an individual's identity
Phishing	A common technique used by threat actors to trick people (typically through e-mails) into divulging personal information, transferring money, or installing malware.
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.
Security-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.
Spoofing	Tricking computer systems or other users by hiding or faking one's true identity. Commonly spoofed targets include e-mails, IP addresses, and websites.
Threat Hunting	A process to proactively and iteratively search for cyber threats through networks that may have evaded existing security measures.
Vulnerability Assessment	A process of identifying, quantifying and prioritising the vulnerabilities of a system, after which vulnerabilities are addressed to prevent exploitation.

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

Cyber incident reporting form:
www.csa.gov.sg/singcert

If you wish to seek scam-related advice:

ScamAlert

Contact anti-scam helpline:
1800 722 6688

Visit ScamAlert website:
www.scamalert.sg

Singapore's Safer Cyberspace Masterplan 2020

ISBN: 978-981-14-7744-7

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

CSA
SINGAPORE