Policy Analysis: Cybersecurity is a Public Good that Starts with the Individual

As of 2016, Singapore has an internet penetration of 82.5% and smartphone penetration of more than 70%. According to a recent survey, Singaporeans spend an average of 3.7 hours online per day on non-work usage, much higher than the regional average. Being connected to such an extent also means an increased exposure to the 'dangers' of cyberspace. Securing Singapore's cyberspace is more than just securing our private and public sector organisations. It must also include the millions of devices owned by the general public that are connected into our nation's infrastructure. If we view cybersecurity as the practice of keeping our digital lives safe and healthy, should the government then treat cybersecurity like public health? This analysis examines the concept of cybersecurity as a public good, whether Singapore should address cybersecurity challenges using a similar approach as it does to public health, and whether it is time to establish a new agency that tackles Singapore's cyber health.

The outbreak of severe acute respiratory syndrome (SARS)[1] in Singapore began in February 2003 when a young woman who had been infected while holidaying in Hong Kong returned to Singapore. When it happened, no one expected a single individual to spread the virus to 238 people and kill 33. More than 20 other countries also reported SARS cases during the global epidemic. Singapore contained the spread of the disease after the implementation of various stringent measures: early detection and isolation, public education, and steps to prevent imported cases. The social and economic impact of SARS is still felt today, and the mere mention of SARS elicits an attentive response from many.

The SARS threat was met with a full and complete response from all quarters: schools, hospitals, public transport operators, airport security, private companies and even hawkers. This was possible because public health is rightly defined as an important public good by the Singapore government.

Today, Singapore is more prepared to tackle any public health epidemic, thanks to lessons learned from the handling of SARS. But could the same be said if Singapore were hit not by a disease like SARS, but by a massive cyberattack?

[1] "Severe Acute Respiratory Syndrome (SARS)," accessed May 13, 2017, http://eresources.nlb.gov.sg/infopedia/articles/SIP_1528_2009-06-03.html.

This case was written by Lim Wei Chieh under the guidance of Tara Thean, Lee Kuan Yew School of Public Policy (LKY School), National University of Singapore and has been funded by the LKY School. The case does not reflect the views of the sponsoring organisation nor is it intended to suggest correct or incorrect handling of the situation depicted. The case is not intended to serve as a primary source of data and is meant solely for class discussion.

Consider this report[2] from the British newspaper The Guardian that ran on Friday, 12 May 2017:

> "Massive ransomware cyber-attack hits nearly 100 countries around the world; More than 45,000 attacks recorded in countries including the UK, Russia, India and China may have originated with theft of 'cyber weapons' from the NSA.
>
> "A ransomware cyber-attack that may have originated from the theft of "cyber weapons" linked to the US government has hobbled hospitals in England and spread to countries across the world.
>
> Security researchers with Kaspersky Lab have recorded more than 45,000 attacks in 99 countries, including the UK, Russia, Ukraine, India, China, Italy, and Egypt. In Spain, major companies including telecommunications firm Telefónica were infected. By Friday evening, the ransomware had spread to the United States and South America, though Europe and Russia remained the hardest hit major companies including telecommunications firm Telefónica were infected."

Cyberattacks do not just cripple systems and structures — they can affect human lives. In the wake of the 2017 ransomware cyberattack, for example, the United Kingdom's National Health Service was forced to cancel operations, divert ambulances to other hospitals, and have its doctors and nurses use pen and paper.[2]

The literature has long drawn parallels between a public health attack and a cyberattack, and extended these parallels to discussions of public health and cybersecurity. This analysis discusses these parallels and offers perspectives and considerations in a Singaporean context.

A nation's `public cyber health' is as much a public good as is its public health. The fallout and socioeconomic impact of a cyberattack is at least as serious for a nation's citizens as an attack by a virus such as SARS on the public health system. Cyberattacks can harm individuals and businesses and even disrupt a nation's essential services (e.g. transport and energy), resulting in significant financial costs to recover from the damages. As such, public cyber health deserves the same investment of resources as that expended to safeguard Singapore's public health system. A good step towards accomplishing this could be for Singapore to have its own `Cyber Health Services' unit.

As of 2016, Singapore has an internet penetration of 82.5% and smartphone penetration of more than 70%. According to a recent survey[3], Singaporeans spend an average of 3.7 hours online per day on non-work usage, much higher than the regional average of 3 hours. Such a high degree of connectivity has its benefits and risks.

As it does in securing Singapore's public health, protecting Singapore's cyber infrastructure involves a whole-of-nation approach that percolates to every level of

[2] Julia Carrie Wong and Olivia Solon, "Massive Ransomware Cyber-Attack Hits Nearly 100 Countries around the World | Technology | The Guardian," *The Guardian*, May 12, 2017, https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs.
[3] Yun Rong Seow, "How Internet Habits Are Affecting Singaporeans' Health, Latest Singapore News - The New Paper," *The New Pap*er, June 12, 2016, http://www.tnp.sg/news/singapore/how-internet-habits-are-affecting-singaporeans-health.

society, touching every community and reaching out to individuals as well as to the millions of mobile devices they own.

How vulnerable is the average person?

Cyberattacks on organisations and institutions, such as the hacking of the Ministry of Defence (MINDEF), the National University of Singapore (NUS) and Nanyang Technological University (NTU) systems, tend to receive a high level of public attention. Unfortunately, the public narrative often starts and ends at the corporate or organisation level. What is left unsaid is that a nation's cyber health depends not just on the security of public and private sector organisations, but also on the security of individual users.

To secure Singapore's smart nation, the security of the millions of connected devices in the hands of Singapore's residents cannot be ignored as they can serve as attack vectors on institutions and critical infrastructure. The strength of any cybersecurity system is dependent on the combined strength of every element in the whole ecosystem — and individual users are often the weakest links in a cybersecurity chain.

A single cyber intrusion on one vulnerable device may appear to harm only a single individual; however, such a breach may act as an attack vector that can bring down a whole security infrastructure. A cyberattack can also involve the malicious intrusion of a population of vulnerable devices together at the same time — the medical equivalent of a pandemic. The national security implications of such an intrusion, if it were to be conducted by a hostile foreign power to attack the nation's critical infrastructure, are chilling.

What, then, is the level of Singapore residents' exposure to the threats and dangers of cyberspace, and how vulnerable are they?

To start, we can examine the level of cyber exposure of Singapore residents by considering the extent of information and communications technology (ICT) adoption, the degree of connectedness to the internet, and the amount of time devices are connected to the internet in Singapore.

Singapore is one of the world's most advanced nations in ICT. Since the early 1980s, the government has embarked on various strategic ICT initiatives and masterplans to bring about economic progress and societal benefits. Today, Singapore ranks number one on the World Economic Forum (WEF) Networked Readiness Index, which measures a nation's ability to leverage ICT for competitiveness and well-being. Singapore has been ranked in the top two positions since 2010.[4]

Singapore is also a highly-connected nation. According to Singapore's Infocomm Development Authority (IDA), 79% of residents age 7 years and above were Internet users and 88% of resident households[5] had internet access in 2015.[6] In addition to being

[4] Baller, Silja (World Economic Forum), Soumitra (Cornell University) Dutta, and Bruno (INSEAD) Lanvin, eds. "The Global Information Technology Report 2016." World Economic Forum, 2016.
[5] Household refers to a group of two or more persons living together in the same house and sharing common food or other arrangements for essential living. It also includes a person living alone or a person

connected at home, Singapore residents are also highly connected when they are on the move. Singapore has a wireless broadband penetration rate of 198.2% as of March 2017.[7] Various studies suggest that Singapore residents spend three to 12 hours daily on their devices. Many devices are connected to the internet for 24 hours a day, even when they are not in active use. As such, this analysis assumes for the sake of discussion that Singaporean devices are typically connected for at least 12 hours a day.

We can thus estimate that 80 to 90% of Singapore residents[8] have access to the internet any time, anywhere using between one to two devices that are connected to the Internet for at least 12 hours a day. We can also estimate that at any point in time, there are around 4.7 million Singaporean devices exposed to the threats and dangers of cyberspace.

How vulnerable are these devices? With such a wide variety of devices and software currently in use, this is difficult to generalise. But all devices can be insecure if the software they are running is not updated with the latest security fixes. Devices can also be insecure if they are not configured correctly, exposing them to potential threats.

To get a sense of the vulnerability problem, let's consider Android (63% of smartphones and tablets as of March 2017) and the Windows operating system (90% of desktops and laptops as of March 2017).[9] According to Google, only half of all Android devices in use at the end of 2016 had received a security update in the previous year.[10] Meanwhile, an average of 7% of Windows systems are unpatched, based on reports[11] by software asset management company Flexera[12]. However, Windows takes the lead with 1,013 vulnerabilities reported in 2016.[13]

The issue of vulnerability becomes especially worrying when we consider that individuals who are not digitally savvy, such as the very young and the very old, are fairly likely to be exposing themselves to cybersecurity threats and dangers. A study conducted by Singapore's then Media Development Authority (MDA)[14] in 2015 showed that 4 in 5 children aged between 0 to 14 years use the internet and go online 4

---

living with others but having his own food arrangements. Although persons may be living in the same house, they may not be members of the same household.

[6] "Infocomm Usage-Households and Individuals - Infocomm Media Development Authority." Accessed April 12, 2017. https://www.imda.gov.sg/industry-development/facts-and-figures/infocomm-usage-households-and-individuals.

[7] "Statistics on Telecom Services for 2017 (Jan - Jun) - Infocomm Media Development Authority." Accessed April 12, 2017. https://www.imda.gov.sg/industry-development/facts-and-figures/telecommunications/statistics-on-telecom-services/statistic-on-telecom-service-for-2017-jan.

[8] Singapore has 3.9 million residents at the end of 2016

[9] "Operating System Market Share." Accessed April 28, 2017. https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0.

[10] "Android Security - 2016 Year In Review," 2016. https://source.android.com/security/reports/Google_Android_Security_2016_Report_Final.pdf.

[11] The Flexera Software Country Reports are based on data from the millions of users of Flexera Software´s Personal Software Inspector. The data includes the average numbers of installed programs — patched and unpatched — on private PCs in the different countries.

[12] "Flexera Software Country Reports." Accessed April 28, 2017. https://www.flexerasoftware.com/enterprise/resources/research/country-reports/.

[13] "Top 50 Products By Total Number Of 'Distinct' Vulnerabilities in 2016." Accessed April 28, 2017. http://www.cvedetails.com/top-50-products.php?year=2016.

[14] MDA has been merged with the Infocomm Development Authority (IDA) to form the Info-communication Media Development Authority (IMDA) as of 1 October 2016

to 6 days a week.[15] According to a 2014 report on device usage among young children, 11% of children between 3-8 years old own their own devices.[16] In a separate study published in 2016 on Southeast Asian kids, 50% of those aged between 6 and 14 own a smartphone.[17]

Should individuals be expected to be aware of the internet's threats and dangers, and to be responsible for their own cyber protection? More importantly, do individuals have the ability to do so? If we acknowledge that protecting the connected devices of individuals will ensure a safer Singapore cyberspace and contributes to national security goals, is it important to invest national resources in safeguarding individual cybersecurity?

To tackle these questions, we should first examine a broader one: Should cyber security be considered a public good?

What is a public good?

A public good is, in theory, one that is both non-excludable and non-rivalrous. This means that the availability of the good to an individual does not exclude others from also enjoying the good, and the use of the good by an individual does not reduce the availability of that good or affect its use by others. For example, law enforcement and national defence, once made available, protect all citizens, and the benefits to one citizen do not reduce the benefits' availability to other citizens. Conversely, a private good such as a shirt becomes unavailable to others once worn by an individual.

In practice, a public good can in fact be excludable if there exists a barrier that prevents an individual from consuming the good. For example, a person is excluded from the benefits of the postal services as a public good if they cannot buy a stamp to post a letter. Some goods, such as roads, are quasi-public goods: as more people use them, their value becomes lower as a result of congestion.

Public goods are an example of a market failure, which is an inefficient allocation of resources in a free market. Private enterprises will not provide public goods in the absence of government intervention — they cannot profit from them when individuals enjoy the benefits of the goods and services for free. If private enterprises were to provide such goods, they would encounter what economists call the 'free rider' problem: the individual who has paid for the consumption of a good or service cannot exclude non-payers from equally enjoying the benefits.

[15] "MDA Zero-to-Fourteen Consumer Experience Study 2015," 2015. https://www.imda.gov.sg/~/media/imda/files/industry%20development/fact%20and%20figures/for%20public%20release%20cs%202015%20final.pdf?la=en

[16] "Mobile Device Usage Among Young Kids," 2014. https://s3-ap-southeast-1.amazonaws.com/tap-sg-media/theAsianparent+Insights+Device+Usage+A+Southeast+Asia+Study+November+2014.pdf.

[17] Menur A. Maulani, Anisa. "Infographic: 50% of Southeast Asian Kids Aged 6 to 14 Own Smartphones." *e27*, January 19, 2016. https://e27.co/infographic-50-of-southeast-asian-kids-aged-6-to-14-own-smartphones-20160119/.

Parallels between public health and cybersecurity

Public health is a public good that focuses on the prevention of disease and the promotion of good health in a population. An individual in a healthy community has fewer chances of contracting a disease and can enjoy good health without diminishing the same benefits to or excluding others. Most governments recognise the importance of public health, and have instituted laws and agencies to manage programs and services that protect citizens' health. In Singapore, the Ministry of Health "believes in ensuring quality and affordable basic medical services for all. At the same time, the Ministry promotes healthy living and preventive health programmes as well as maintains high standards of living, clean water and hygiene to achieve better health for all".[18]

Like public health, cybersecurity is a public good: it is both non-excludable and non-rivalrous. We cannot exclude individuals in a network from the benefits of a secure cyberspace, and an individual who benefits from the cybersecurity of a network does not reduce the opportunity for others to also benefit.[19]

Cybersecurity may not be a pure public good, however. The vibrant private sector devoted to providing cybersecurity services and solutions demonstrates a profit-driven motive. While the efforts of private enterprises may produce public benefits, they are unlikely to reach the state's desired levels of cybersecurity. As such, government intervention is still required.[20] On the other hand, it is also possible that the lively private sector is a result of government intervention in the form of grants, incentives and investments for cybersecurity enterprises and large-scale public sector procurement of cybersecurity products and services.

The state of public health and cybersecurity are both heavily dependent on environmental factors. The environment in which an individual resides is an important factor when considering harm to either physical or digital health. The World Health Organisation (WHO) notes that environmental factors are a root cause of most disease, death and disability, accounting for 25% of death and disease globally. In a cyber environment, an individual is similarly vulnerable to environmental factors in the form of computer viruses, cyberattacks and other digital menaces through his or her connected digital device.

Public health and cybersecurity both encounter and are influenced by interdependencies between individuals. Viruses, which are present in both the physical and cyber environments, are an example of this. Healthy individuals and those who are vaccinated are more resistant to viruses and less likely to spread diseases. Similarly, in cyberspace, a 'healthy' connected device is more resistant to computer viruses and therefore less likely to be hacked into and used to breach and infect or hack other connected devices. In both cases, 'public health' is secured.

---

[18] "Our Healthcare System | Ministry of Health." Accessed May 2, 2017. https://www.moh.gov.sg/content/moh_web/home/our_healthcare_system.html.

[19] Schneider, Fred B (Cornell University), Elaine M (UC Berkeley) Sedenberg, and Deirdre K (UC Berkeley) Mulligan. "Public Cybersecurity and Rationalizing Information Sharing." International Risk Governance Center, 2016.

[20] Powell, Benjamin. "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry," 2001. http://www.independent.org/pdf/working_papers/57_cyber.pdf.

There is evidently a spillover benefit to others in cyberspace when an individual invests in cybersecurity to prevent loss or damage. However, since the benefits of securing a single device may not accrue fully to the individual, the level of cybersecurity that an individual applies may be less than optimal for reaping public benefits. The individual may perceive the cost of cybersecurity to be higher than the private benefits; also, individual users may not be convinced that they have to secure their mobile devices fully for the sake of public good. Thus, government may need to intervene by either reducing or offsetting the cost to the individual to achieve the desired level of public cybersecurity benefits.[14]

Drawing a parallel between health and cybersecurity is nothing new. Many of our approaches towards cybersecurity are modelled after health care measures. Public heath aims to identify and monitor health threats, prevent diseases and injuries before they occur, and diagnose conditions in early stages for easier treatment. Similarly, in recent years, both the public and private sectors in cybersecurity have renewed their focus on the identification and monitoring of cyber threats, early detection of cyberattacks and rapid response to contain and mitigate the impact of cyberattacks.

If cybersecurity plays a key role in maintaining safe and healthy digital lives for Singapore's residents, cybersecurity should be treated in a similar way as is public health. Is it time to establish a 'Singapore Cyber Health Services' agency to provide quality and affordable basic cybersecurity services?

The Possibilities of a Singapore Cyber Health Services Agency

According to the Bloomberg Global Health Index, Singapore is the fourth healthiest country in the world. The index grades each country based on variables such as life expectancy, causes of death and health risks ranging from high blood pressure and tobacco use to malnutrition and the availability of clean water.[21] While there are likely to be numerous contributing factors to Singapore's high standing, Singapore's Ministry of Health recognises that rising standards of living, high standards of education, good housing, safe water supply and sanitation, high quality medical services and the active promotion of preventive medicine have significantly improved the health of Singapore residents.[22]

Some critical features of most public health laws and programmes include the following:[23]

1. Public education: Creating awareness and understanding to enable an individual to take ownership of their own health, including programmes aimed at educating the population about the causes, effects and prevention of diseases;

[21] Lu, Wei, and Vincent Del Giudice. "Italy's Struggling Economy Has World's Healthiest People - Bloomberg." *Bloomberg Markets*, March 20, 2017. https://www.bloomberg.com/news/articles/2017-03-20/italy-s-struggling-economy-has-world-s-healthiest-people.
[22] "Singapore Health Facts | Ministry of Health." Accessed April 12, 2017. https://www.moh.gov.sg/content/moh_web/home/statistics/Health_Facts_Singapore.html.
[23] Mulligan, Deirdre K, and Fred B Schneider. "Doctrine for Cybersecurity." *Daedalus* 140, no. 4 (2011): 70–92. doi:10.2307/23046915.

2. Prevention and treatment: Establishing measures to prevent and treat specific diseases, including mandates for vaccinations, a steady supply of medicines, provision of subsidies for the needy and compliance with health and hygiene standards;

3. Surveillance and analysis: Identifying and managing diseases and infected individuals, including mandatory reporting for specific diseases and conditions, testing and screening of individuals exhibiting certain symptoms, and quarantine requirements.

For cybersecurity, the country could adopt a similar set of features while keeping in mind Singapore's healthcare financing philosophy of "universal healthcare coverage to our citizens, with a financing system anchored on the twin philosophies of individual responsibility and affordable healthcare for all".[24]

Specifically, this analysis suggests three programmes that could help improve and maintain the cyber health of Singapore residents. The programmes focus on educating the young and vulnerable, reducing the vulnerabilities of connected devices and making cybersecurity affordable for the masses.

1. Cybersecurity curriculum for primary schools

In 2017, Singapore's Cyber Security Agency (CSA) launched the first national cybersecurity awareness campaign, "Live Savvy with Cybersecurity". Unlike previous initiatives targeted at businesses, the roadshow attempted to educate the general public on the importance of 'good cyber hygiene' to secure their online activities.[25]

While this was an important initiative, a more formal approach — one similar to that adopted for health education — to inculcate a stronger understanding of cybersecurity from a young age may be worthwhile. For decades, health education has been a part of the syllabus for primary schools in Singapore. Besides promoting messages based on key health risks identified by Singapore's Health Promotion Board, this early education provides young children with the knowledge and skills to take responsibility for their own health, the health of others and the environment.

Primary school children should be educated on the basics of cybersecurity to promote awareness of the threats and dangers they might encounter when connecting to the internet. The CSA could work with the Ministry of Education's (MOE) Curriculum Planning and Development Division to roll out a syllabus that progressively introduces different aspects of cybersecurity over the six years of primary school education. In addition to classroom and laboratory lessons, the curriculum could also include field trips to visit the Singapore government's Cyber Watch Centre (CWC).

[24] "Costs and Financing | Ministry of Health." Accessed May 4, 2017. https://www.moh.gov.sg/content/moh_web/home/costs_and_financing.html.
[25] "CSA Launches First National Cybersecurity Awareness Campaign," 2017. https://www.csa.gov.sg/news/press-releases/csa-launches-first-national-cybersecurity-awareness-campaign.

2. Cyber ‘vaccinations’ for Singapore citizens

The rampant spread of malicious software (malware), especially ransomware, is one of the biggest cyber threats faced by consumers today. Unlike governments and businesses with the resources to defend themselves, consumers may not have sufficient ability to protect their connected devices. Greater government support may be needed to help Singapore citizens ‘vaccinate’ themselves against such cyber threats.

Public health receives robust governmental support in Singapore. Singapore’s National Childhood Immunisation Programme (NCIP) covers immunisations against a list of life threatening diseases, and it is compulsory for every child to receive diphtheria and measles immunisations under Singapore’s Infectious Diseases Act. The government fully subsidises all recommended immunisations under the NCIP for Singaporean children with the exception of Pneumococcal vaccines, which can be paid for using Medisave (see “Cyber health screenings and care”). The NCIP has proven to be an effective means for sharply reducing incidences of targeted diseases. Singapore’s Ministry of Health (MOH) also provides subsidies for drugs approved under the Standard Drug List (SDL) and Medication Assistance Fund (MAF) at public hospitals, specialist outpatient clinics and polyclinics to ensure that patients have access to effective medications for common medical conditions.[26]

Instead of diseases, cyberspace has to reckon with malicious software (malware) — an umbrella term for viruses, worms, ransomware, spyware, and so on. Malware is created by people with malicious intent, including criminals, terrorists and hostile nation states, and can attack in different ways, including stealing your information, manipulating your financial transactions, and taking control of your device to attack other connected devices in cyberspace. According to the Microsoft Security Intelligence Report (SIR), Volume 21, one in five computers in Singapore reported a malware issue in the second quarter of 2016.[27] A 2016 report by the Singapore Police Force stated that while violence, housebreaking and other related crimes in Singapore dropped to a 20-year low in 2015, online commercial crimes were up by 95%.[28]

Anti-malware solutions are the equivalent of vaccines against malware threats. Such solutions can help to prevent malware infections and also detect, contain and eradicate malicious software. Most people are aware of antivirus software and many install free versions on their devices. Still others may have enabled a firewall, which provides another layer of defence. While such basic solutions are better than nothing, they are quite inadequate in today’s hostile cyber

[26] “Drug Subsidies & Schemes | Ministry of Health.” Accessed May 5, 2017. https://www.moh.gov.sg/content/moh_web/home/costs_and_financing/schemes_subsidies/drug_subsidies.html.
[27] “One in Five Computers in Singapore Reported a Malware Encounter in 2Q2016: Microsoft Report,” February 6, 2017. https://news.microsoft.com/en-sg/2017/02/06/one-in-five-computers-in-singapore-reported-a-malware-encounter-in-2q2016-microsoft-report/#sm.0001i01y26myydunuun2iuzrvkqzy%23IszGaBJfUW04WsoI.97.
[28] Othman, Liyana. “Singapore’s Crime up 4% in 2015, Driven by Cybercrime.” *Channel NewsAsia*, February 12, 2016. http://www.channelnewsasia.com/news/singapore/singapore-s-crime-up-4-in-2015-driven-by-cybercrime-8177276.

environment. Today, a new virus can spread rapidly and infect millions of machines before the antivirus companies even know it exists or get a chance to prepare a signature update — and even if they prepare an update, the companies must still wait for the users to update the antivirus software. This means that antivirus companies are always playing catch up. Viruses can also mutate, or new variants can quickly be created to evade the detection of signature antivirus software.

The government could consider providing a free commercial solution similar to the NCIP for malware, and subsidizing more advanced add-ons for Singapore citizens.

3. Cyber health screenings and care

In Singapore, multiple tiers of assistance and financing help ensure that Singapore citizens have access to basic healthcare.[21] The same level of thinking should be applied to securing the cyber health of individuals. Below are examples of healthcare-related assistance and financing to which Singaporeans are entitled.

- Subsidies: The government subsidizes up to 80% of the total bill in acute public hospital wards.

- Medisave: This is a compulsory medical savings scheme contributed by working Singapore citizens and their employers, which helps with the financing of medical treatment.

- Medishield Life: A basic health insurance plan, aimed at large hospital bills and selected costly outpatient treatments, whose premiums are kept affordable by a range of government subsidies.

- Medifund: The government has a medical endowment fund that provides financial assistance for needy Singapore citizens. For example, the Community Health Assist Scheme (CHAS) subsidizes medical and dental care for Singapore Citizens from lower- to middle-income households.

In addition, from September 2017, eligible Singapore residents have access to health screening for diabetes, high cholesterol, high blood pressure, obesity, colorectal cancer and cervical cancer under the Health Promotion Board's (HPB) Screen For Life programme.[29] The cost is S$5 at clinics under the CHAS scheme, S$2 for CHAS cardholders and free for Singapore's Pioneer Generation.[30]

Just as the HPB has been driving home the message that health screening is important, we need to encourage Singapore residents to assess the cyber health

[29] Khalik, Salma. "Parliament: Flat $5 Health Screening Fee for Eligible Singaporeans." *The Straits Times*, April 5, 2017. http://www.straitstimes.com/politics/parliament-flat-5-health-screening-fee-for-singaporeans-above-40.

[30] Singapore's Pioneer Generation refers to Singapore citizens that are aged 16 and above in 1965 and obtained citizenship on or before 31 December 1986. This is the generation of pioneers that built Singapore as a nation.

of their devices on a regular basis. The screening can help determine if software is updated to fix known vulnerabilities and whether connected devices are configured appropriately to minimize exposure to cyber threats. There are different mechanisms, such as the distribution of free tolls for users to self-perform the assessment, that the government could consider.

When we suffer from symptoms of ill health, we typically visit the doctor. A similar norm should be considered for cybersecurity. The difference is that 'treatment' may not need to be administered physically, but could be delivered online, depending on the specific situation faced by the users. Just like a visit to the doctor, increased contact with 'cyber health' professionals helps raise the overall awareness of 'cyber health' issues and promotes deeper understanding and appreciation of what one should or should not be doing to protect their 'cyber health'.

The above suggested programmes are by no means exhaustive. Other areas deserving of consideration include quarantine in times of 'cyber' outbreaks, proof of 'immunisation' when connected into Singapore's internet infrastructure, and other equivalent public health measures. Just like Singapore's health care system, not all programmes and services can and should be administered by the government, and intermediaries like internet service providers (ISPs) will have a role to play in improving the country's cybersecurity.

Conclusion

Today, internet connectivity is so ubiquitous that a 2011 United Nations report[31] declared internet access to be a human right, and that disconnecting people from the internet is a human rights violation and against international law. Health is also a human right. The United Nations Universal Declaration of Human Rights[32] states that "everyone has the right to a standard of living adequate for the health and well-being of himself and of his family". Governments thus have a responsibility to ensure both good public health and a safe cyberspace for their citizens. Approaching cybersecurity with a similar mindset as that towards public health as well as establishing relevant public services to ensure sound cyber health will lay a solid foundation for a safer Singapore.

[31] La Rue, Frank. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue," 2011. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[32] "Universal Declaration of Human Rights | United Nations." Accessed May 7, 2017. http://www.un.org/en/universal-declaration-human-rights/.