

2020

CYBERSECURITY

TECH ACCORD

PROTECTING USERS & CUSTOMERS EVERYWHERE

CYBERSECURITY

AWARENESS

IN THE COMMONWEALTH OF NATIONS

A PROJECT BY THE CYBERSECURITY TECH ACCORD
AND THE U.K.'S FOREIGN & COMMONWEALTH OFFICE



Foreign &
Commonwealth
Office



The Commonwealth



EXECUTIVE **SUMMARY**

In 2019, the Cybersecurity Tech Accord and the United Kingdom's Foreign and Commonwealth Office have collaborated in developing this report as part of an ongoing partnership to better understand and promote cybersecurity awareness across the Commonwealth of Nations (the Commonwealth). It provides a brief introduction to both the Cybersecurity Tech Accord and the Commonwealth, including a snapshot of cybersecurity preparedness and awareness efforts across the member-state organisation.

It also explores the different ways in which countries across the Commonwealth are choosing to promote cybersecurity awareness in their local contexts, highlighting the types of activities being pursued. This includes national campaigns, workshops, competitions and digital resources, among others. The appendix then provides a high-level overview of cybersecurity awareness initiatives in respective countries in the Commonwealth.

The report is not intended to provide a ranking of national awareness efforts or cybersecurity preparedness, or to evaluate the effectiveness of respective cybersecurity awareness programs. Instead, the report is intended to provide helpful resources for those looking to further develop cybersecurity awareness programs within their own countries based on the learnings and efforts of others in the Commonwealth. Nevertheless, it does include high level guidance from the Cybersecurity Tech Accord on the five characteristics of effective efforts to promote cybersecurity awareness. Such programs should be *current, recursive, inclusive, culturally responsive and multistakeholder* in nature. One initiative the report strongly encourages all nations to adopt is the recognition of October as *Cybersecurity Awareness Month* – a simple and helpful way to join with countries from around the world in raising the profile and importance of cybersecurity awareness.

In the spirit of collective learning, this report marks the end of one phase of this project and the beginning of another. In addition to sharing the findings of our work, the Cybersecurity Tech Accord looks forward to facilitating further dialogue and providing additional support to Commonwealth nations seeking to improve cybersecurity awareness over the next year, in the form of workshops and the sharing of additional resources to improve efforts to raise awareness.

Finally, should Commonwealth governments want to contribute further information on awareness programs that is not currently reflected in this report, we encourage them to please reach out to the Cybersecurity Tech Accord secretariat (info@cybertechaccord.org), or the Commonwealth Cyber Programme (Tehrime.Khan@fco.gov.uk) so that later editions of this report can reflect additional input and a more complete picture of the activities taking place.

INDEX

- 01. EXECUTIVE SUMMARY
- 03. INTRODUCTION
- 04. THE CYBERSECURITY TECH ACCORD – AN INDUSTRY COMMITMENT
- 05. THE COMMONWEALTH OF NATIONS
- 06. METHODOLOGY AND APPROACH
- 07. THE IMPORTANCE OF CYBERSECURITY AWARENESS
- 13. SNAPSHOT: CYBERSECURITY PREPAREDNESS AND AWARENESS ACROSS THE COMMONWEALTH OF NATIONS
- 17. CYBERSECURITY AWARENESS MONTH – AN INTERNATIONAL MOVEMENT FOR ALL
- 20. AWARENESS INITIATIVES IN THE COMMONWEALTH OF NATIONS
- 33. APPENDIX – COMMONWEALTH COUNTRY OVERVIEWS
- 34. COMMONWEALTH NATIONS IN AFRICA
- 38. COMMONWEALTH NATIONS IN ASIA
- 40. COMMONWEALTH NATIONS IN THE CARIBBEAN & SOUTH AMERICA
- 43. COMMONWEALTH NATIONS IN EUROPE & NORTH AMERICA
- 44. COMMONWEALTH NATIONS IN OCEANIA

INTRODUCTION

We live in an increasingly connected world, where networked technologies are more than ever interwoven with our daily lives, improving and enhancing the ways in which we conduct business, monitor our health, receive services, and connect with one another. This exciting trend is only growing, with more communities in more nations coming online each year and joining the greatest experiment in human history – the Internet. However, alongside the myriad benefits of this resource, which makes the wealth of human knowledge available at the stroke of a key, come new risks and new responsibilities for keeping ourselves safe.

The rapid expansion of Internet access alongside the proliferation of network-connected devices including smartphones, tablets, wristwatches and even household appliances – the so-called Internet of Things (IoT) – have increased the avenues and methods by which malicious actors can seek to harm technology users. These cyber threats can be easy to overlook, when adopting new technologies that seamlessly integrate into and improve our everyday activities, but the danger they pose is only increasing with a growing threat surface. In fact, estimates suggest that cyberattacks will likely cost the global economy in the trillions of dollars in the coming years.¹

While there are many steps the technology sector and governments can take to reduce cyber risk, the best line of defence against cyberattacks has always been the awareness of end users of how to be responsible consumers of technology products and services. Time and again, studies confirm that the vast majority of cyberattacks rely on simple human error by an end user – clicking on a malicious link, downloading suspicious software, etc. These types of attacks can be defended against by practicing basic cybersecurity hygiene and maintaining awareness of the threats that exist online. However, such awareness needs to be intentionally built.

This is why the Cybersecurity Tech Accord is proud to join with the United Kingdom's Foreign and Commonwealth Office (FCO) to explore the state of cybersecurity awareness across the Commonwealth, identifying successes, as well as opportunities for growth, and providing industry insights. This partnership builds on the cooperative relationship between Microsoft and the FCO to support greater cybersecurity awareness. The cultural, geographic and socioeconomic diversity in the Commonwealth, which includes some of the world's most advanced cybersecurity powers, as well as nations coming online for the first time, provides a unique opportunity to explore a range of cybersecurity awareness needs. Meanwhile, the common bonds between these nations creates an opportunity for collective sharing, learning and action to drive greater cybersecurity awareness.

In an increasingly connected world, in which we all share the same cyberspace, improvements in cybersecurity are never zero-sum. Harms in one geographic region can, and frequently do, spread to others quite rapidly. Similarly, improvements in cybersecurity are also shared. This is a collective challenge to promote cybersecurity awareness, and when one nation wins, we all win.

¹ <http://www.mckinsey.com/business-functions/business-technology/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks>

THE CYBERSECURITY TECH ACCORD — AN INDUSTRY COMMITMENT

The Cybersecurity Tech Accord is a global coalition of technology companies committed to improving cybersecurity for users and customers around the world by adhering to four foundational cybersecurity principles for the technology industry.

- I. We will protect all our users and customers everywhere
- II. We will oppose cyberattacks on innocent citizens and enterprises from anywhere
- III. We will help empower users, customers and developers to strengthen cybersecurity protection
- IV. We will partner with each other and likeminded groups to enhance cybersecurity

Launched with 34 company signatories in April of 2018, the Cybersecurity Tech Accord today includes over 130 company signatories, from more than twenty countries across four continents. More than just a statement, signatories of the agreement meet regularly to identify opportunities for collaboration to improve the cybersecurity of an online world that connects more people and organisations across the globe every day. Grounded in the four principles, signatories have endorsed and supported norms and frameworks, provided input to policymaking efforts, and led by example on issues like vulnerability disclosure. In addition, the Cybersecurity Tech Accord has pursued, and supported initiatives meant to develop the cybersecurity capacity of communities and organisations everywhere.

Celebrating Cybersecurity Awareness Month

October is Cybersecurity Awareness Month and provides a great opportunity each year for the Cybersecurity Tech Accord to share resources and guidance to keep technology users informed about how to stay safe online. Last year, during the first October after launching the Cybersecurity Tech Accord, the group released a set of its top-10 tips for securing your online environment, a handy guide featuring the most critical steps users can take to avoid falling victim to cyberattacks.

These capacity building efforts are aligned with the third principle of the Accord – *We will help empower users, customers and developers to strengthen cybersecurity protection* – and underscores the responsibility the technology industry has for supporting users and customers in understanding how to use technology products and services safely and to minimise vulnerability to cyber risk. As the world continues to become more connected with emerging economies coming online for the first time, and technology continues to make remarkable advancements each year, citizens everywhere must be empowered to consider not only "how do I use this?" but more importantly "how do I use this responsibly?"

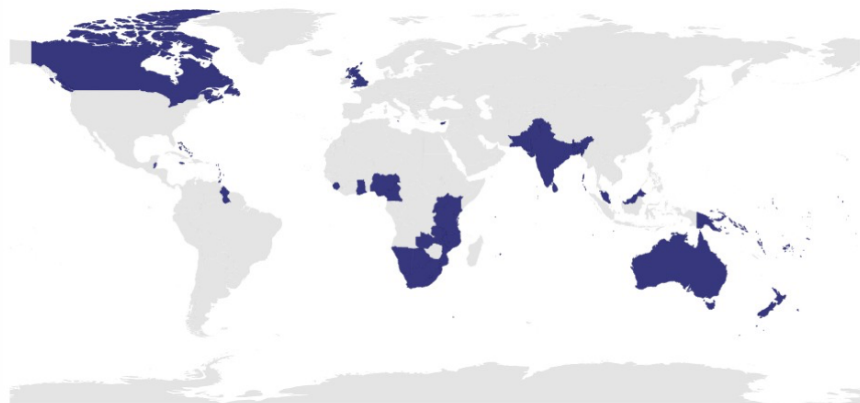
THE COMMONWEALTH OF NATIONS

The Commonwealth of Nations is an international organisation made up of 53 member-states around the world. Existing beyond any one region, the Commonwealth is a coalition that spans five continents, with its membership bound together by shared cultural and historical experiences. Through respective Commonwealth offices in each country, and the Commonwealth Secretariat acting as the main intergovernmental agency and central institution, the network identifies areas for collaboration and cooperation for their collective advancement.

The Commonwealth is a diverse network to say the least, representing approximately one-quarter of the countries in the entire world, and resists any easy generalisations. It includes some of the world's most advanced economies - including Australia, Canada, and Singapore - as well as many emerging economies. The Commonwealth also boasts some of the most populous nations within its membership, most notably India's 1.3 billion people, as well as some of the smallest countries like the Pacific Island nations of Nauru and Tuvalu.² However, while there are marked geographic, cultural and economic differences, this very diversity is the organisation's greatest asset, as the structures put in place by the Commonwealth can facilitate a rapid exchange between respective nations on a wide range of topics, allowing all member states to learn from one another and identify the best practices that work for them on any number of issues.

The Commonwealth includes more than one-fourth of the countries on earth, including some of the largest and smallest.

The Commonwealth of Nations, Member Countries



<https://thecommonwealth.org/member-countries>

² The Commonwealth, Member Countries. <http://thecommonwealth.org/member-countries>. Commonwealth Secretariat. 2019.

METHODOLOGY AND APPROACH

This report was developed throughout the course of 2019, leveraging several different approaches to cultivate data about levels of cybersecurity preparedness and awareness initiatives across the Commonwealth. This included a desk review of publicly available material from each of the respective Commonwealth governments, national data collected as part of indices maintained by the International Telecommunications Union (ITU)³ and the National Cyber Security Index,⁴ as well as the deployment of an original survey developed by the Cybersecurity Tech Accord focused specifically on cybersecurity awareness initiatives and activities across the Commonwealth. A draft of the report was also released online via the Cybersecurity Tech Accord Website for public comment and further contributions in October of 2019. All of this information is intended to help understand the state of cybersecurity awareness in the Commonwealth and the different types of programs pursued to promote further awareness.

The authors appreciate all of the contributions from outside parties that have made this report possible, including from officials from Commonwealth states. This summative report presents the findings from this study and has several central goals:

- I. Deliver a snapshot of overall cybersecurity awareness efforts across the Commonwealth;
- II. Highlight unique approaches to cybersecurity awareness taken by respective governments, or groups of governments, in the Commonwealth for mutual learning;
- III. Provide recommendations on cybersecurity awareness initiatives that have proved effective from the perspective of the technology industry;
- IV. Encourage recognition of October each year as Cybersecurity Awareness Month, throughout the Commonwealth, and,
- V. Set the stage for further dialogue and engagement between Commonwealth nations, and with the Cybersecurity Tech Accord, on how to cultivate persistent and meaningful cybersecurity awareness.

Unlike other efforts to collect information on cybersecurity policies or capacities, this report does not seek to create any particular index or ranking of cybersecurity awareness programs or initiatives in the Commonwealth or elsewhere. Promoting greater awareness of any new, complicated issue is challenging, whether it is related to public health, technology, or any other topic, and needs to be culturally responsive to respective national contexts. Therefore, this report merely seeks to share what initiatives have been pursued and what has been effective in different countries in hopes that it can inform the approaches of other nations. There

³ ITU. *Global Cybersecurity Index (GCI)*, 2018. ITU Publications. Geneva, Switzerland. 2019. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

⁴ NCSI: National Cyber Security Index. e-Governance Academy Foundation. Tallinn, Estonia. <https://ncsi.ega.ee/>

is no "winner" when it comes to cybersecurity awareness. In a networked world, risks and vulnerabilities are inherently shared, and so too are gains and improvements.

In that spirit of collective learning, this report marks the end of one phase of this project and the beginning of another. In addition to sharing the findings of our work, the Cybersecurity Tech Accord looks forward to facilitating further dialogue and providing additional support to Commonwealth nations seeking to improve cybersecurity awareness over the next year, in the form of workshops and the sharing of additional resources to improve efforts to raise awareness. In addition, should Commonwealth governments want to contribute further information on awareness programs that is not currently reflected in this report, we encourage them to please reach out to the Cybersecurity Tech Accord secretariat (info@cybertechaccord.org), or the Commonwealth Cyber Programme (Tehrime.Khan@fco.gov.uk) so that later editions of this report can reflect additional input and a more complete picture of the activities taking place.

THE IMPORTANCE OF CYBERSECURITY AWARENESS

WHAT IS CYBERSECURITY?

Before exploring the importance of cybersecurity awareness, it is necessary to first clarify what we mean by *cybersecurity*, as this is a term that is understood differently in different contexts. For the purposes of this report we will leverage a helpful and comprehensive definition provided by Cisco Systems, a Cybersecurity Tech Accord signatory:

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.⁵

In other words, cybersecurity is about protecting digital systems from attacks that would corrupt or otherwise exploit them to cause harm, either to the systems themselves or in the physical world. This is meaningfully different from a discussion about what information should or should not be shared over digital platforms. Though discussions of content restrictions – what people should and should not be allowed to share or express online – are also important, this report is focused exclusively on how to avoid the corruption and exploitation of technology itself, taking into account contemporary security trends and threats and how to mitigate them.

Cybersecurity is a relatively new challenge, one that has only truly developed with the advent of the modern Internet and all the devices it connects today. Despite that, cybersecurity increasingly impacts every individual, organisation and government on the planet. However, while cybersecurity

⁵ Cisco Systems. What is Cybersecurity? <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>

is a shared challenge, it is also one that impacts societies quite differently: with costs and damages from attacks varying widely from region to region, country to country and even from one organisation to another. This is readily apparent from even a cursory look at available data.

One can compare, for example, the 8% of mobile devices in Singapore estimated to be infected with malware at any given time, to the 36% of such devices that are compromised in Bangladesh – a 450% increase in infection rate within the same geographic region.⁶ Similarly, according to reports, Internet users in Ukraine are 23 times more likely to fall victim to a crypto mining attack as their peers in Denmark.⁷ The implications from these statistics are quite clear – while cyberattacks and cybercrime are inherently borderless assaults, individuals and organisations in some countries are much less likely to be victimised than those in others. Borders may not matter to attackers, but they seem to make a difference when it comes to who is harmed.

There are many explanations for why cybersecurity outcomes can vary so widely from one nation to another, many variables that factor into how vulnerable any individual user, organisation or country is to an attack. This includes the technology products that are predominantly used, the cybersecurity policies and regulations that have been implemented, the sophistication of cloud and other infrastructure, geopolitical rivalries – the list goes on. However, despite the myriad contributing factors, one major determinant of overall cybersecurity is consistently found to be the level of awareness by end users.

What is Cybersecurity Awareness?

If cybersecurity is about threats to digital systems, cybersecurity awareness refers to the knowledge of users about these threats, and their ability to practice habits to recognise and avoid them. This includes foundational things, like how to identify a phishing scam, knowing to not use untrusted USB sticks, changing default access information and using sufficiently complex passwords, as well as limiting who has access credentials. Beyond simply understanding and being able to identify and avoid these threats, cybersecurity awareness also includes knowing where and how to report suspicious activity when it occurs. In an increasingly connected world, this type of awareness is as critical as knowing to look both ways before crossing a busy street.

95% of cybersecurity breaches are due to errors by end users

– such as failing to identify a phishing email.

⁶ Moody, Rebecca. *Which countries have the worst (and best) cybersecurity?* Comparitech. Feb. 6, 2019. Kent, UK. <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/>

⁷ Ibid

While the importance of cybersecurity awareness is perhaps no surprise, its critical significance is remarkable when considering just some of the available statistics:

- 95% of all cybersecurity breaches are due to some form of human error by the end user.⁸
- More than 90% of successful hacks are the result of phishing attacks.⁹
- Investment in human awareness training can immediately reduce cybersecurity risk for an organisation by more than 50%.¹⁰

The evidence is quite clear, attackers tend to focus their efforts on "weak links" – this includes individuals who lack the awareness of how to operate with proper "cybersecurity hygiene," good security habits and practices, to keep themselves and their organisations safe.

While there are many things that the technology industry can and is doing to create more secure products and services and that governments can do by adopting appropriate policies, nothing can replace the impact of a healthy culture of cybersecurity awareness. Such a culture needs to be deliberately built across each level of a society: within communities, businesses, municipalities, nations and even in our international engagements with one another. This is why governments around the world have been pursuing cybersecurity awareness campaigns and initiatives to help keep their citizens safe – oftentimes in partnerships with civil society and the private sector. These programs can take many different forms, including setting aside particular time to recognise the importance of cybersecurity, like during a Cybersecurity Awareness Month. They can also be focused on promoting awareness with different target groups, such as youth populations, small businesses or the elderly, among many others.

⁸ Milkovich, Devon. *13 Alarming Cyber Security Facts and Stats*. Cybint Cyber Solutions. Dec. 3, 2018. <https://www.cybintsolutions.com/cyber-security-facts-stats/>

⁹ 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics. Cisco and Cybersecurity Ventures. Feb. 2019. <https://cybersecurityventures.com/cybersecurity-almanac-2019/>

¹⁰ *New Research from Aberdeen Group and Wombat Security Confirms Security Awareness and Training Measurably Reduces Cyber Security Risk*. Proofpoint. 2015. <https://www.wombatsecurity.com/press/press-releases/research-confirms-security-awareness-and-training-reduces-cyber-security-risk>

CYBERSECURITY AWARENESS INITIATIVE EXAMPLES¹¹

KIRIBATI

"The Government is actively engaging in cybersecurity awareness campaigns targeting children, parents and guardians. The content of the campaigns include the risks associated with young people and their access to the internet, including malware awareness & safety tips, grooming, identity theft, and how to become digital citizens. The Government is also working closely with Cyber Safety Pasika in efforts to protect children in the cyberspace domain."

MALTA

"The Cyber Security Malta Campaign was launched in October 2018. It is the national campaign that focuses on raising awareness and promoting education on cybersecurity. The campaign has various target audiences such as academia, the public sector, the private sector, techies and the general public. Initiatives and respective topics vary by audience and the cybersecurity risks at the time of planning. The delivery method used in implementing the initiatives is meticulously chosen to ensure effectiveness amongst the respective target audience."

ZAMBIA

"The 'Train the Trainer' initiative is a program that is delivered as a two day workshop and targets primary and secondary school teachers to impart child online protection knowledge and cybersecurity awareness in them that the trained teachers are then expected to share with children within their jurisdictions... the aim is to conduct this workshop in each of the ten provinces of Zambia."

¹¹ Examples are quoted from national responses to a survey conducted between August and September 2019 on cybersecurity awareness by the UK Foreign and Commonwealth Office and the Cybersecurity Tech Accord

QUALITIES OF EFFECTIVE CYBERSECURITY AWARENESS PROGRAMS

The next several sections of this report will highlight different approaches governments in the Commonwealth are taking to promote a culture of cybersecurity awareness among their citizens. These examples include public awareness campaigns, educational initiatives, trainings and digital resources, as well as other approaches. And while all of these examples can provide helpful lessons and insights for those considering how to further promote awareness in their own country, it is important to first understand what makes for effective cybersecurity awareness efforts. The Cybersecurity Tech Accord recommends national awareness programs try and reflect the following five characteristics:

- **Up-to-date.** Unlike other public awareness issues, cyber threats evolve quickly alongside each new innovation in technology. As a result, efforts at promoting cybersecurity awareness need to make sure they are sharing the information citizens need to know, based on current threats. While some best practices may persist, such as regularly updating software, others will necessarily change in line with evolving threats.
- **Recursive.** Cybersecurity is not a task to be completed and set aside, but rather something individuals and groups need to be constantly aware of while they are using technology products and services. Therefore, cybersecurity awareness initiatives should be pursued with regularity to keep citizens mindful of cyber risk, and to be continually building and reinforcing a culture of cybersecurity.
- **Inclusive.** There should be no question in the minds of policymakers about who needs to be aware of cybersecurity best practices – *we all do*. In a connected world, anyone who is using products and services on a network needs to be aware of how to do so responsibly, both for their own security and the security of others. This includes youth demographics as soon as they are interacting with technology products, as well as the elderly. The need for awareness cuts across all professions and social strata, and includes the most technologically savvy, as well as those who are coming online for the first time.
- **Culturally responsive.** While we increasingly all connect to the same public Internet, the ways in which we do – including the devices we use and rules for doing so – vary widely from country to country. As important, the ways in which we use modern technology and the way we learn new information is heavily influenced by local customs and cultures. With this in mind, cybersecurity awareness initiatives cannot be one-size-fits-all, but should rather be tailored to the needs and customs of a particular country.
- **Multistakeholder.** Promoting greater cybersecurity awareness is a responsibility that should be shared across all stakeholder groups in collaboration with one another. Governments should of course be

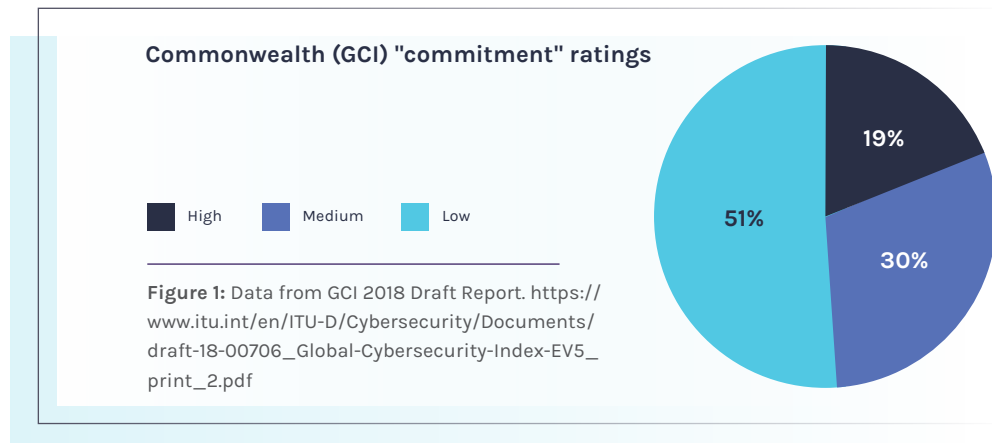
invested in promoting greater awareness among their citizens and are best positioned to lead these efforts. Meanwhile, the technology industry and relevant civil society organisations are often uniquely suited to understanding what information the public needs to know, as they are responsible for building and maintaining the technology in the first place.

The remainder of this report works to highlight the state of cybersecurity awareness efforts in the Commonwealth, and to provide a taxonomy of approaches and illustrative examples from member states. However, for those seeking tactical guidance on how to develop particular cybersecurity awareness programs, we recommend exploring the good practices and guidance materials made available by the Global Forum for Cybersecurity Expertise (GFCE), (available here: <https://www.thegfce.com/good-practices/cyber-security-awareness>), as well as consulting the resources catalogued in the GFCE's new knowledge sharing portal for cybersecurity capacity building, "Cybil" (available here: <https://cybilportal.org/>).

SNAPSHOT: CYBERSECURITY PREPAREDNESS AND AWARENESS ACROSS THE COMMONWEALTH OF NATIONS

The diversity of the Commonwealth clearly comes across in the level of cybersecurity investment, preparedness and awareness in the region. This section provides a high-level overview of this dynamic based on the data collected as part of global indices. Further information about individual countries and their cybersecurity awareness measurements and capacities is available in the appendix of this report.

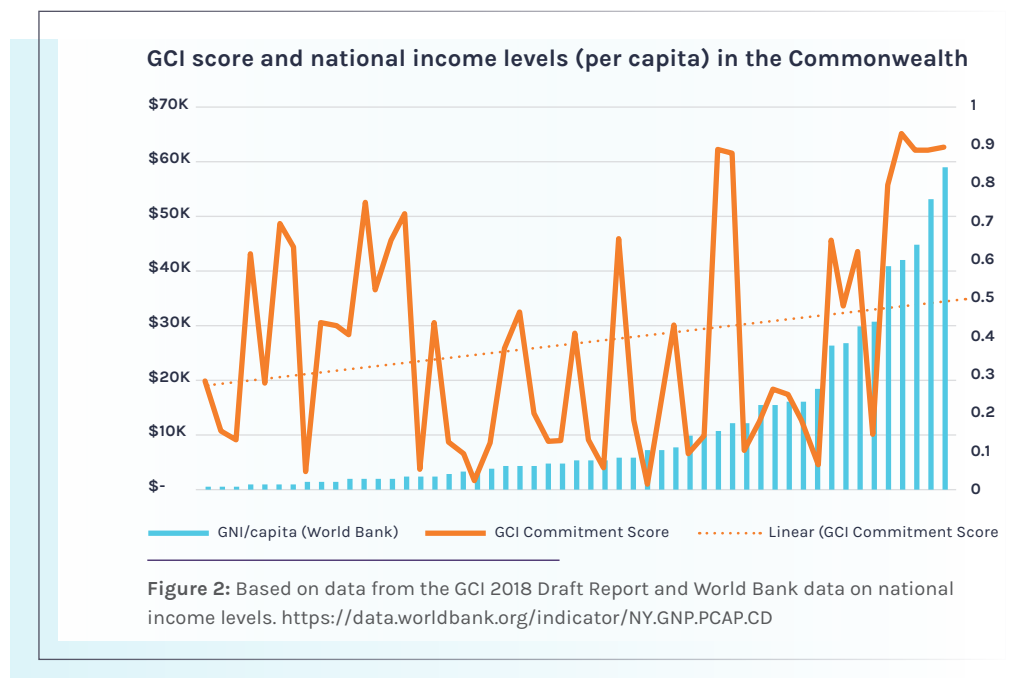
To get a sense of how this association of countries breaks down in regards to overall cybersecurity capacity, the Global Cybersecurity Index (GCI), developed and maintained by ITU, provides an overall "cybersecurity commitment" rating based on measurements of legal, technical, organisational, capacity building, and cooperation indicators. Based on this summative rating, nations are then sorted by whether they have a "High," "Medium," or "Low" level of commitment to cybersecurity. The breakdown of Commonwealth countries by this "commitment" rating is reflected in the chart below.



As can be seen in Figure 1, a slight majority of Commonwealth countries are rated in this index as having a "low" commitment to cybersecurity. However, it should be noted that this distribution largely mirrors the global breakdown of cybersecurity commitment ratings. The United Kingdom has the highest score of any country in the cyber commitment ratings, and other Commonwealth states – Australia, Singapore, Canada and Malaysia – are in the top 10 as well. Of all 194 nations included in the GCI, 45% were rated "low," 28% were "medium," and 27% were "high" in overall cybersecurity commitment.¹² This largely parallel breakdown in ratings distribution makes the Commonwealth ideal to focus on in this study of cybersecurity awareness promotion, as it can serve as an example of how such efforts can be scaled to other nations that have similar needs as well.

¹² GCI, 2018.

Unsurprisingly, nations with more resources have been more likely to invest in cybersecurity capacities and awareness efforts. For example, high and upper-middle income Commonwealth countries are more than twice as likely to have primary or secondary cybersecurity education programs in place than low and low-middle income Commonwealth countries, based on World Bank ratings.^{13,14} Similarly, Commonwealth countries with higher per capita incomes have, on average, a higher GCI commitment rating. However, and importantly, this correlation is hardly predictive and there are many examples of low and low-middle income countries in the Commonwealth with high GCI commitment scores – indicating that a country does not need to be wealthy to improve their cybersecurity. This is illustrated in Figure 2 below, which organises all 53 Commonwealth countries from least to greatest income per capita (blue bars) and then indicates their corresponding GCI score (orange line).



¹³ GNI per capita, Atlas method (current US\$). The World Bank Group. 2019. <https://data.worldbank.org/indicator/NY.GNP.PCAP.CD>

¹⁴ Prydz, Espen Beer, Divyanshi Wadhwa "Classifying countries by income." The World Bank Group. Sept. 9, 2019. <https://datatopics.worldbank.org/world-development-indicators/stories/the-classification-of-countries-by-income.html>

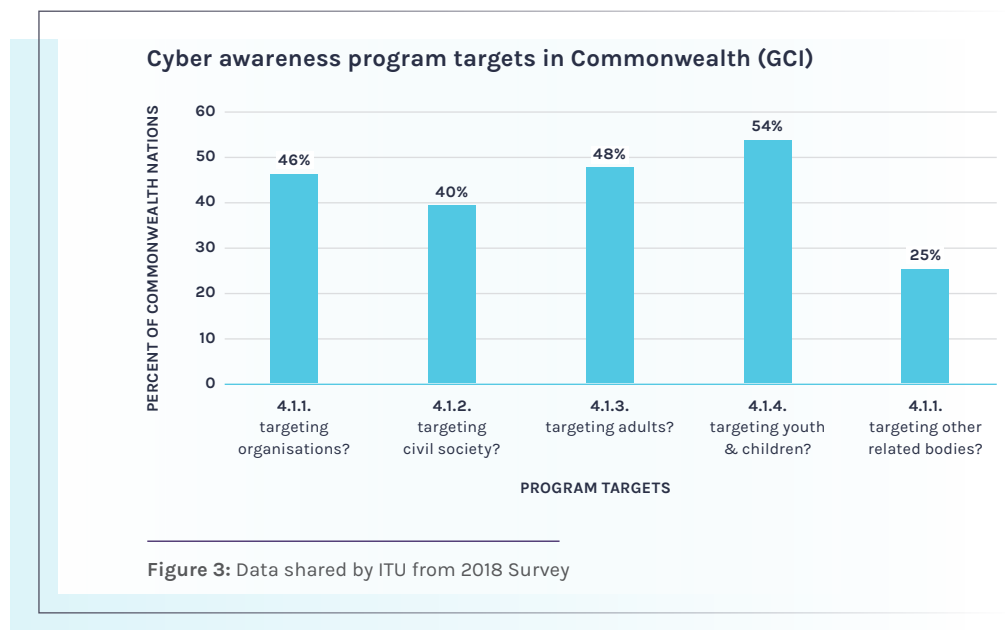
Nearly 40% of Commonwealth countries

reported having no cybersecurity awareness programs in 2018.

CYBERSECURITY AWARENESS PROGRAMS IN THE COMMONWEALTH

Drilling down further into the GCI dataset, there are additional insights related to cybersecurity awareness in particular. According to the survey data, when asked specifically if "Public awareness campaigns have been developed and implemented?" 21 Commonwealth countries reported having no such cybersecurity awareness programs in place - nearly 40% of the entire Commonwealth.^{15 16}

The demographics that Commonwealth countries then responded as having targeted in their cybersecurity awareness initiatives are reflected in Figure 3 below. From the data, it is clear that countries are taking different approaches and prioritising a variety of targets populations in these efforts. However, while "children & youth" are receiving the most attention in these efforts, awareness programs targeting them exist in only slightly more than half of Commonwealth nations, according to this data. And for all other demographics provided, awareness initiatives exist in less than 50% of Commonwealth countries.

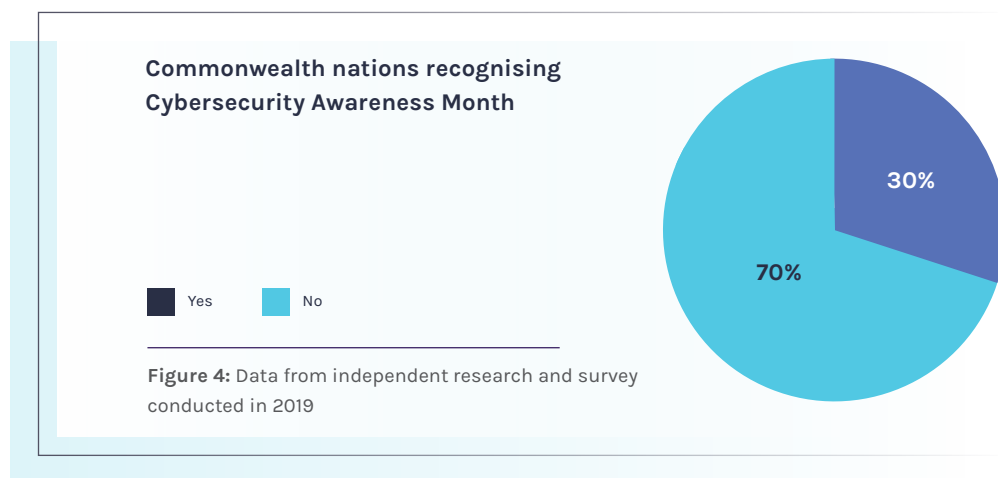


One leading way in which many countries across the globe have started spearheading public awareness efforts around cybersecurity has been by joining in designating October as "Cybersecurity Awareness Month." This month-long commemoration has received widespread support in large part thanks to international campaigns led by US, Canadian, and EU diplomatic

¹⁵ GCI, 2018.

¹⁶ It should be noted that in our independent research we were able to identify awareness programs in over 40 Commonwealth countries - though many were managed by private entities or international organisations.

efforts encouraging more nations to adopt the initiative. However, while many nations have joined in this global movement, 70% of Commonwealth nations have yet to do so, based on the research for this report (Figure 4). The following section explores Cybersecurity Awareness Month in more depth, how different countries have approached it and what its potential benefits are.



CYBERSECURITY AWARENESS MONTH – AN INTERNATIONAL MOVEMENT FOR ALL

A number of Commonwealth nations, though not yet a majority, have joined in a growing global effort to recognise October as "Cybersecurity Awareness Month" each year. A simple but effective concept, Cybersecurity Awareness Month is an annual public campaign that sets aside the month of October to focus on educating citizens about how to stay safe online. Nations that recognise the month generally have a government agency or authority responsible for facilitating and coordinating events and engagements throughout the month to highlight the importance of cybersecurity awareness and to focus on areas of particular concern. In addition, private sector partners, and even other governments, that recognise the month often collaborate in developing and supporting programming for it.

Activities for a National Cybersecurity Awareness Month (NCAM) can include simple messaging efforts, based on things like hashtags and slogans, as well as more in-depth events including workshops focused on particular cybersecurity challenges or target audiences. Nations have different approaches to implementing NCAM, with many choosing to divide the month into week-long segments, each with a different theme, while others focus more on providing resources and empowering local governments and other partners to leverage them as needed during the month. While Cybersecurity Awareness Month is just one example of a public campaign on awareness, its structure is consistent with all of the principles previously outlined for responsible cybersecurity awareness initiatives – *up-to-date, recursive, inclusive, culturally response, and multistakeholder*.

Less than 1/3 of Commonwealth Nations

have recognised
Cybersecurity
Awareness Month

Cybersecurity is not a box to be checked and set aside, it is something that needs to be continually practiced and performed to keep pace with evolving threats. Establishing NCAM as an annual event ensures that efforts to promote cybersecurity awareness are revisited regularly and updated with information to reflect current challenges and what citizens need to know to be safe. As a global effort, adopted on a national basis, NCAM is intended to involve citizens at every level of a society and organisations across sectors, and allow governments to customise their approaches based on national needs and contexts. Finally, as you will see from the examples below, recognising NCAM can also serve as a rallying cry for multistakeholder support, drawing attention from governments, industry and civil society organisations to cooperate in promoting cybersecurity awareness at the same time.

The following examples highlight just a few different approaches national governments have taken to observing a National Cybersecurity Awareness Month in October.

- **United States** – Coordinated by the National Initiative for Cybersecurity Careers and Studies (NICCS), NCAM in the US is organised around annual themes, in 2019 it emphasised user responsibility under the slogan "Own it. Secure it. Protect It." In addition, NICCS provides an annually updated toolkit on its website with resources and information on current cybersecurity challenges to support those around the country who want to host events in support of Cybersecurity Awareness Month.¹⁷
- **European Union** – The European Union has successfully advocated for the adoption of October as Cybersecurity Awareness Month across all of its member states. Events and activities for NCAM in the EU are coordinated by the European cybersecurity agency (ENISA) based on different themes chosen each year. Past themes for the EU's cybersecurity awareness month have included "recognising cyber scams" and "emerging technologies and privacy."¹⁸
- **Canada** – Managed by the government's "Get Cyber Safe" program, Canada maintains an online dashboard with shareable resources aligned to the themes of NCAM each year. Last year's themes addressed a diversity of audiences, with topics including "how cyber threats work," "how cyber threats affect you," "how to protect yourself online," "how to protect your small business," and "how to work together."¹⁹
- **Australia** – As part of Australia's NCAM recognition, the nation's Cyber Security Centre and Centre for Defence Industry Capability has partnered with regional governments to sponsor a series of presentations highlighting priority cybersecurity issues facing small businesses in particular.²⁰

Recognising October as a shared NCAM in nations around the world also underscores the nature of cybersecurity challenges – they are shared. In an interconnected world, it is fitting that the same time period be set aside each year to collectively recognise how peoples of all nations can continue to be better stewards of a communal cyberspace, setting up further opportunities for cooperation moving forward. Especially for countries that have not yet pursued other cybersecurity awareness initiatives, and where there may be limited institutional capacities for doing so, recognising NCAM in October is a great first step to promote awareness and join a global campaign. However, as previously mentioned, recognition of NCAM across the Commonwealth is currently limited and, as the chart below indicates, while there is universal

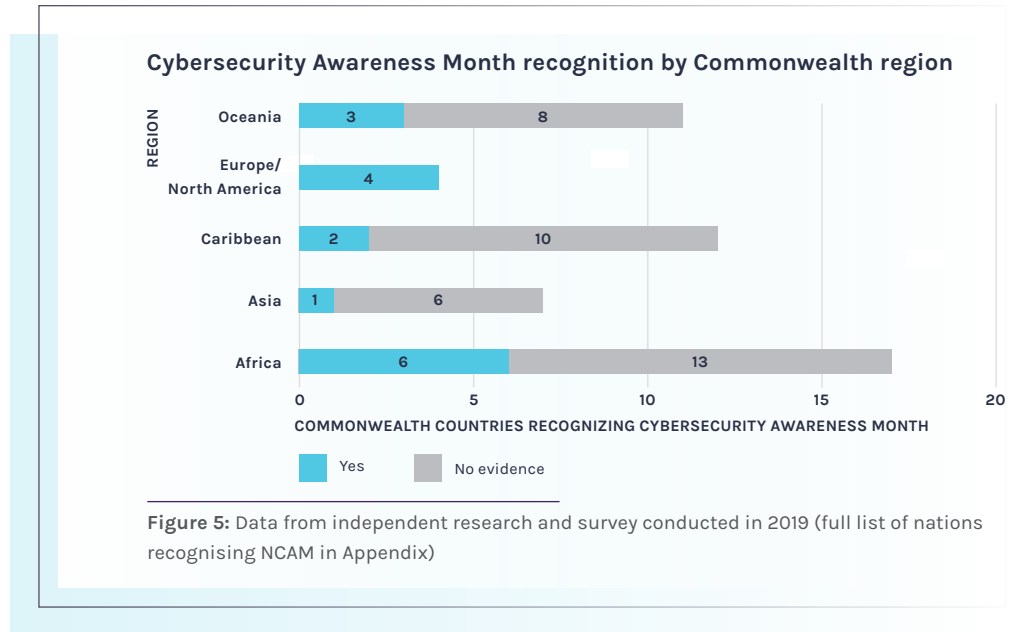
¹⁷ National Cybersecurity Awareness Month 2019. National Initiative for Cybersecurity Careers and Studies. Nov. 15, 2019. <https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019>

¹⁸ European Cyber Security Month 2018. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/events/european-cyber-security-month-2018>

¹⁹ Cyber Security Awareness Month Toolkit. Government of Canada. <https://www.getcybersafe.gc.ca/cnt/rsrscs/csam-tlkt-en.aspx>

²⁰ Cybersecurity Awareness Month. Northern Territory Government. September 2018. <https://business.nt.gov.au/news/2018/cyber-security-awareness-month>

adoption among Commonwealth states in Europe and North America, adoption in other regions remains low.



In the following section, there are descriptions of other types of cybersecurity awareness initiatives that are pursued in Commonwealth member states, and it should be noted that recognising Cybersecurity Awareness Month often presents a good opportunity to amplify or further promote the messages of these other campaigns during a time of national attention.

AWARENESS INITIATIVES IN THE COMMONWEALTH OF NATIONS

This section provides examples of approaches taken by different countries, or groups of countries, throughout the Commonwealth to promote cybersecurity awareness. The programs are grouped according to various characteristics, including how they are delivered, their duration, and other structural elements:

- I. national awareness campaigns,
- II. awareness workshops,
- III. digital resources hubs,
- IV. hackathons/competitions,
- V. cybersecurity awareness organisations, and
- VI. cybersecurity awareness education.

In this section we also introduce concrete examples of how different countries choose to implement cybersecurity awareness approaches. These examples are not intended to provide an exhaustive overview of all such efforts taking place, but will hopefully leave the reader with a sense of what implementation can look like in practice. It is important to note that while we group the initiatives based on their common characteristics, this categorisation does not mean they are the only area of focus a particular country is investing in. Many nations are pursuing multiple cybersecurity awareness activities at the same time and blending the categories below within broader initiatives. For example, cybersecurity workshops and national awareness campaigns often coincide strategically with Cybersecurity Awareness Month, as a way of bringing more attention to the issue at an optimal time.

Each of these approaches provides a unique way to increase cybersecurity awareness. They highlight the different possible ways to improve cybersecurity hygiene, taking into account national priorities, as well as cultural and economical differences. We hope that the categorisation, and in particular the examples provided, enable other actors to learn about new possible approaches and use them in their own work.

NATIONAL CYBER AWARENESS CAMPAIGNS

Several nations in the Commonwealth have implemented ongoing national campaigns intended to promote and reinforce cybersecurity awareness. These types of campaigns, which are also popular for promoting things like public health or public safety, are helpful in directing national attention towards a pressing topic for a sustained period of time. They can indicate to a broad audience that an issue – in this case cybersecurity – is an urgent priority of which the public should take notice and be aware. These campaigns generally try and create simple messaging on a particular issue intended to reach a wide audience, and can include things like public awareness announcements, such as targeted advertisements, and public

remarks made by elected officials at a national level, but may also try and target specific communities.

While national campaigns and associated mass communications may not be ideal for more nuanced messaging, they can create the auspices for events and gatherings that do provide deeper dives on particular issues. The recognition of Cybersecurity Awareness Month is one form of national awareness campaign that provides such opportunities. As highlighted in the previous section, in addition to developing catchy slogans like the United States' "Own IT. Secure IT. Protect IT." and "#BeCyberSmart," Cybersecurity Awareness Month can be used to highlight specific issues via workshops and new resources. In fact, all of the subsequent types of initiatives and activities included here to promote cybersecurity awareness – workshops, resource hubs, competitions, organisations, and curricular materials – can be, and often are, important parts of broader national cybersecurity awareness campaigns.

The examples provided below of national awareness campaigns in the Commonwealth highlight some of the different approaches countries have taken to developing and communicating messages on cybersecurity awareness at a national level.

Examples throughout the Commonwealth:

1

Eswatini: National Cybersecurity Awareness Month

2019 was the first year that Eswatini observed a National Cybersecurity Awareness Month. The event was coordinated by the nation's Ministry of ICT which organised the month into four distinct weeks that each focused on a different cybersecurity theme: online safety, social media, fraud awareness, and child safety. In addition to creating downloadable resources and guidance materials for each theme, the month's activities also included a series of school visits and industry workshops, as well as national advertisements to reinforce the campaign messaging.

More information: <https://www.esccom.org.sz/cybersecurity/>

2

Malta: National Cyber Security awareness and educational campaign

Malta launched a 2-year cybersecurity awareness campaign in 2018. The campaign is intended to keep the public better informed about cyber risks as an increasing amount of daily interactions move online. The campaign is deliberately intended to reach across social strata in the country to make sure everyone is aware of best practices for staying safe online. The campaign began with a public survey to establish a baseline understanding

3

of cybersecurity awareness and where critical gaps may exist. The campaign also recognised October as "Cybersecurity Awareness Month" in Malta.

More information: <https://mita.gov.mt/en/ict-features/Pages/2018/Launch-of-a-National-Cyber-Security-awareness-and-educational-campaign.aspx>

United Kingdom: Security Awareness Campaigns

In the UK, the Centre for the Protection of National Infrastructure (CPNI) has put together a series of toolkits for awareness campaigns focused on specific security topics – including about phishing attacks and monitoring one's "digital footprint." Each campaign includes a series of downloadable materials to allow it to be implemented independently by organisations, especially those responsible for national infrastructure.

More information: <https://www.cpni.gov.uk/security-awareness-campaigns>

NATIONAL CYBERSECURITY AWARENESS WORKSHOPS

Cybersecurity awareness workshops are becoming increasingly common events, where governments and other organisations bring together key stakeholders at a particular time and place to better understand and promote public awareness of how to stay safe online. Often sponsored in partnership with private sector organisations, these workshops allow for a more in-depth discussion of particular gaps in cybersecurity awareness and how they can be addressed. They can also be focused on reaching out to and including specific stakeholder groups or populations that are most in need of improved cybersecurity awareness. As compared to national awareness campaigns, awareness workshops are generally singular events drawing attention to particular issues that may require greater depth or attention to address. However, awareness workshops can certainly be incorporated into broader national awareness campaigns.

Importantly, the impact and effectiveness of cybersecurity awareness workshops is as dependent on who attends as on the quality of their content. A workshop may be focused on promoting awareness among civil society organisations, financial sectors, or in primary school classrooms, to name a few; but in each instance it will be important to have the right leaders and influencers in attendance from these groups to ensure the messages of the workshop are both received and shared more broadly. Failure to have the right people in the room at these events can blunt the impact of an otherwise well-developed workshop when the resources and knowledge provided are not amplified or communicated any further. A particular type of these workshops – a "training of the trainers" event – focuses on not just providing information to attendees, but also specifically on equipping them to share the content of the workshop further.

The examples from the Commonwealth below highlight how these workshops are often developed in collaboration between governments and other stakeholders – including the private sector – as well as with other governments. One prominent example is the UK's Get Safe Online program, which has been hosting a series of awareness raising workshops in partnership with Commonwealth governments across the Caribbean.

Examples throughout the Commonwealth:

1

Belize: National Cyber Security Symposium

This week-long workshop in Belize is hosted by several governmental offices with sponsorship from corporate partners. The workshop focuses on promoting awareness of the current cyber threats among essential stakeholders. The week kicks off by recognising a "National Cybersecurity Awareness Day."

More information: <https://cybersecurity.nigf.bz/>

2

Brunei: Cyber Security Forum

This gathering is hosted by the Royal Brunei Technical Services, with sponsorship from a private sector partner. It focuses on facilitating greater awareness among corporations about contemporary cyber threats and ways organisations can operate safely online.

More information: <https://www.rbts.com.bn/iet-visit-to-rbts-training-simulation-centre-tsc-2/>

3

Caribbean: Get Safe Online Awareness Workshops

Get Safe Online, a digital resource platform sponsored by the UK government, has been focused on sharing its resources and guidance regarding online safety in Commonwealth nations across the Caribbean. Leveraging their online resources, the organisation has hosted dedicated workshops in St. Kitts & Nevis, Guyana and Barbados, with plans for further public engagement across the other 9 nations.

More information: https://www.getsafeonline.bb/themes/site_themes/getsafeonline/resources/GSO_Commonwealth_Press_Kit_October_19.pdf

DIGITAL RESOURCE HUBS

National campaigns and initiatives can only do so much to share critical messaging on cybersecurity awareness with citizens. As a result, many nations are increasingly hosting content on cybersecurity awareness on government websites. While the Internet is awash with resources highlighting cybersecurity best practices, government investment in developing and hosting native resources provides a number of benefits. First, citizens can be more confident that the information provided is credible, current and coming from a reliable source. Second, the material available can be provided in the local language and responsive to local contexts and trends as it relates to cybersecurity. Finally, governments can leverage an ongoing platform to provide updated information on cyber threats and best practices as it sees fit, and differentiate the content provided, focusing on particular sectors or demographics as needed. Many of the examples included below are targeted specifically at youth, consumers, small businesses, or other specific audiences.

Maintaining a web presence with accurate and timely information on cybersecurity awareness requires time and resources on behalf of governments, as well as effective communication to constituent groups to let them know that the resources exist, where to find them and when they are updated. It can therefore be helpful to leverage national campaigns and workshops to direct traffic to these resources, which also allow for a deeper dive into any awareness concerns highlighted in a national campaign. It should also be noted that while there is benefit to government engagement and support in these efforts, digital resource hubs can also be managed by independent organisations and NGOs focused on promoting cybersecurity awareness. In fact, the Cybersecurity Tech Accord maintains an ever-growing virtual webinar series of its own on a range of current cybersecurity topics. The series is developed in partnership with the Global Forum for Cyber Expertise (GFCE), serving as a valuable free resource that is available here: <https://cybertechaccord.org/webinars/>.

As with other cybersecurity awareness raising efforts, digital resource hubs benefit from the inclusion of industry and other multistakeholder insights, in partnership with governments, to ensure the information provided is accurate and up-to-date, while also responding to national needs and local contexts. The examples of digital resource hubs below show reflect a range of approaches – with some hosted directly by government agencies and others by independent organisations.

Examples throughout the Commonwealth:

1

Mauritius: General Information Security Guidelines

The Mauritius Computer Emergency Response Team (CERT) maintains a web presence with a "Knowledge Bank" that includes "General Information Security Guidelines" to support awareness on cybersecurity issues among citizens. The website includes reference materials on antivirus best practices, device security, social media privacy, and web browser security.

More information: http://cybersecurity.ncb.mu/English/Knowledge_bank/Pages/Guidelines.aspx

2

South Africa: Cyber Tips & Advice

South Africa's Telecommunications and Postal Service maintains a website with digital resources to help familiarise citizens the common cybersecurity threats and how to avoid them.

More information: <https://www.cybersecurityhub.gov.za/cyberawareness/index.php/cyber-tips-advice.html>

3

Trinidad and Tobago: CyberSafe TT

This website providing awareness resources, largely for parents and students, includes cybersecurity guidance materials focused on youth still in primary school. CyberSafeTT is a private organisation, but has collaborated to produce its video series on common cybersecurity threats with the Telecommunications Authority of Trinidad and Tobago

More information: <http://cybersafett.com/>

4

United Kingdom: Get Safe Online

Sponsored by government agencies in the United Kingdom, in partnership with many from across the private sector, Get Safe Online is a comprehensive online portal hosting curated resources for individuals, families and businesses on how to safely navigate the online world. It has specific subsections on protecting devices, personal information and children online, as well as how to responsibly use online services like banking and social networks.

More information: <https://www.getsafeonline.org/>

5

United Kingdom: NCSC's Information for...

This online content hub is hosted by the UK's National Cyber Security Centre and includes resources targeted at individuals and families, businesses of all sizes, public entities and even cybersecurity professionals. The website is regularly updated with current information and the range of resources available for each target group includes preventative advice as well as guidance on what to do if/when an individual or organisation finds themselves compromised by an incident.

More information: <https://www.ncsc.gov.uk/section/information-for/>

HACKATHONS/CYBERSECURITY COMPETITIONS

Particularly in nations with more advanced cybersecurity cultures, "hackathons" or open cybersecurity competitions can be a great way to generate both new interest and innovative ideas for addressing cyber threats by inviting a diversity of perspectives and backgrounds into the conversation to help solve problems. These competitions can be structured to focus on a particular topic, or simply invite proposals for addressing cybersecurity challenges more broadly. Similarly, they can be designed to target narrow populations – like graduate students in certain fields – or open to whomever would like to participate. While not exclusively focused on promoting basic cybersecurity awareness, these hackathons can nevertheless generate greater awareness, understanding, and engagement among non-traditional populations in tackling cybersecurity challenges.

Today's cybersecurity challenges require greater awareness by all technology users, and they also require innovative thinking to develop and socialise new solutions. This is an additional benefit of cybersecurity contests and competitions, which can invite participation and collaboration across disciplines and among underrepresented groups that may not have otherwise considered how their backgrounds and expertise could help improve cybersecurity. The Cybersecurity Tech Accord launched one such contest in December of 2019, calling on teams of young individuals from across the globe to develop new technology solutions that improve peace and stability online (more information: <https://cybertechaccord.org/cybersecurity-tech-accord-announces-new-contest-in-partnership-with-the-un-office-of-disarmament-affairs/>). The examples below from Commonwealth nations in particular highlight how these programs help stimulate interest among underrepresented groups based on age, gender, or other lines of difference.

Examples throughout the Commonwealth:

1

Australia: Cyber Security Challenge

The Cyber Security Challenge Australia (CyCSA) is an annual program facilitated by Australia's Cyber Security Centre and supported by a host of partners from the private sector and academia. The program is targeted at university students with an emphasis on gender inclusiveness. Participants are divided into teams of four and tasked with navigating real-world cybersecurity challenges.

More information: <https://www.cyberchallenge.com.au/>

2

Australia: Cyber Security Challenges Dashboard

Beyond any one competition, the Australian Cyber Security Growth Network (AustCyber) maintains a dashboard cataloguing cybersecurity challenges and competitions that Australian citizens can participate in, both domestically and in more than a dozen countries around the world. The dashboard allows for searches by geography and format, and includes the CyCSA Challenge above, as well numerous others.

More information: <https://www.austcyber.com/node/106>

3

United Kingdom: CyberFirst Girls Competition

This annual competition, focused on supporting girls in primary school interested in cybersecurity careers, is sponsored by the UK's National Cyber Security Centre in coordination with local school districts across the country. The competition has teams of four work on customised cybersecurity challenges designed to align with the UK's computer science curricula. No prior IT expertise is required and the program is intended to facilitate creative and divergent problem solving.

More information: <https://www.ncsc.gov.uk/section/cyberfirst/girls-competition>

CYBERSECURITY AWARENESS ORGANISATIONS

Nearly all the cybersecurity awareness programs described in this report rely on the coordination and leadership of designated officials, and often require cooperation between different agencies, as well as with external stakeholders in the private and non-profit sectors. Therefore, many nations have established organisations dedicated to coordinating cybersecurity awareness as an essential part of their mandate. These organisations can

be structured in different ways: some are part of dedicated cybersecurity agencies operated by governments, others are housed as parts of other departments, while still others exist as organisations that operate entirely independent from their national government.

Promoting national cybersecurity awareness requires a sustained and ongoing commitment to building and maintaining a culture of cybersecurity. To this end, it is helpful and important to have a dedicated organisation that take responsibility to coordinate a multifaceted approach to building cybersecurity awareness, evaluating the progress of respective programs, and identifying the gaps within public awareness that should be further addressed. The below examples from the Commonwealth illustrate how a few countries have organised their entities responsible for promoting cybersecurity awareness.

Examples throughout the Commonwealth:

1

Canada: Get Cyber Safe

This program is operated within the Canadian Centre for Cyber Security and serves as the primary public interface for the organisation, whose mandate includes promoting cybersecurity awareness. Get Cyber Safe maintains a website with a wealth of digital resources on how to avoid common cybersecurity threats and is also responsible with coordinating a robust set of activities and engagements during Cybersecurity Awareness Month each October.

More information: <https://www.getcybersafe.gc.ca/index-en.aspx>

2

Singapore: Cyber Security Awareness Alliance

The Cyber Security Awareness Alliance is an association led by the Infocomm Development Authority of Singapore, which includes partners from both the public sector and private industry working to raise awareness of cybersecurity issues and encourage the adoption of best practices among users. The Alliance hosts a wealth of digital resources on their website for individuals and businesses alike, and also coordinates awareness campaigns and events focusing on different audiences and cybersecurity topics.

More information: <https://www.csa.gov.sg/gosafeonline>

3

The Gambia: Cyber Security Alliance

This private organisation operating in The Gambia provides ongoing training on cyber threats and cybersecurity best practices to organisations from public, private and non-profit sectors, including trainings for law enforcement officials and activists.

More information: <http://gamcybersecurityalliance.com/>

4

Commonwealth Telecommunications Organisation

The Commonwealth Telecommunications Organisation (CTO) has a broad mandate to support the development and use of ICTs for social and economic advancement across the Commonwealth of Nations. To that end, one of its strategic priorities is "cybersecurity," including a focus on cyber hygiene. In addition to coordinating activities and events across the commonwealth, their website hosts helpful materials and curricular resources intended to improve cyber hygiene.

More information: <https://www.cto.int/strategic-goals/cybersecurity/cyber-hygiene/>

5

Ghana: National Cyber Security Centre

In Ghana, the nation's cybersecurity agency plays a lead role in promoting awareness via several recurring initiatives. This includes leading and coordinating events alongside Cybersecurity Awareness Month, as well as the ongoing "A Safer Digital Ghana Programme" which has awareness initiatives targeted at different demographic groups - including for children, the general public, and businesses.

More information: <https://cybersecurity.gov.gh/index.php/a-safer-digital-ghana-programme/>

6

Guyana: National Data Management Authority, Computer Incident Response Team

While many nations today have a dedicated computer incident response team (CIRT) to manage preparations and operations in the aftermath of a cyber incident, Guyana's CIRT also includes a mandate to focus on "promotion of cybersecurity issues and awareness nationally."

More information: <https://ndma.gov.gy/pillars/cybersecurity/>

7

Malaysia: CyberSAFE

CyberSAFE Malaysia is the public outreach arm of the cybersecurity agency in the country, it is focused on facilitating the communication of cybersecurity priorities with the broader public. This includes programs focused on the awareness needs of kids, youth, adults and organisations. CyberSAFE has curricular resources for schools, online reference materials on its website, and also hosts a cybersecurity competition through its school outreach program.

More information: <https://www.cybersafe.my/en/>

8

New Zealand: NetSafe

NetSafe is an independent non-profit operating in New Zealand focused on promoting awareness of online safety issues facing children and youth. Among other initiatives, the organisation is advocating for recognition of a "Safer Internet Day" in New Zealand in February of 2020, which it has promoted in the past along with supporters from public organisations, civil society and private industry.

More information: <https://www.netsafe.org.nz/>

9

Rwanda: National Agency for Information and Communication Technologies

In Rwanda, the national cybersecurity agency operates within its mandate to also provide cybersecurity awareness trainings and resources to targeted populations in the country. This includes regionally specific cybersecurity awareness trainings and direct engagements with local schools across the country. The agency also hosts guidance materials on its website on a wide range of cybersecurity topics to improve awareness.

More information: https://rwandacybersec.org/?page_id=87

CYBERSECURITY AWARENESS EDUCATION

Governments can make substantial improvements in general levels of cybersecurity awareness by ensuring that a basic introduction to online safety is part of their national education system. As students are expected to increasingly use technology as part of their academic careers, and indeed throughout their lives, requisite training on how to stay safe in doing so should be a core component of any curriculum. Curricular resources for incorporating cybersecurity education into classroom settings – including

educational standards, as well as lessons plans and supporting materials – are increasingly being developed by government agencies as well as by independent organisations to be leveraged at all school levels, from primary through university, and even continuing adult education.

Further guidance on how to develop and implement an effective cybersecurity curriculum go beyond the scope of this report – and indeed would easily fill a separate and worthwhile study – but the importance of such programs for building a culture of cybersecurity nevertheless warrants brief recognition here. The examples below illustrate just a few of the types of curricular resources that are being developed in Commonwealth countries to serve learners of all ages and needs.

Examples throughout the Commonwealth:

1

South Africa: South African Cyber Security Academic Alliance (SACSAA)

SACSAA is a collaboration between different academic institutions across South Africa focused on developing free educational resources to promote cybersecurity awareness among youth populations. They have developed a dedicated cybersecurity curriculum for children in primary school and facilitate school visits on request to provide lessons on cybersecurity awareness for students and staff at both primary and secondary schools in South Africa.

More information: http://www.cyberaware.org.za/?page_id=520

2

Australia: Schools Cyber Security Challenges

Developed in partnership between multiple Australian agencies and private sector entities, the Schools Cyber Security Challenges provides a series of immersive learning experiences, intended for high school students, focused on topics like data sharing, personal information security, and cryptography. Beyond simply providing classroom materials, the program has also rolled out a series of roadshows and professional development opportunities to help teachers prepare to incorporate the curriculum in their classrooms.

More information: <https://aca.edu.au/projects/cyber-challenges/>

3

United Kingdom: Essential Digital Skills Framework

In the UK, the Department for Education has now developed multiple iterations of its "Essential Digital Skills Framework," highlighting educational standards for adults to safely participate in the digital economy. This effort stands out for its commitment to include adult learners in the Department for Education's efforts to support employers and educational institutions across the UK that provide trainings on digital safety.

More information: <https://www.gov.uk/government/publications/essential-digital-skills-framework>

APPENDIX — COMMONWEALTH COUNTRY OVERVIEWS

The following section provides an overview of the cybersecurity capacities and resources that exist within each respective Commonwealth country and that could support the development of greater cybersecurity awareness. The information provided below is based on a desk review of materials made available by government agencies, data contained in the GCI and NCSI indices, as well as the direct responses of government officials to a survey developed and conducted by the FCO and Cybersecurity Tech Accord. In order to avoid misstating which programs or initiatives exist within each country, an indication of "N/A," or "not available" does not mean that the program or entity does not exist, only that we could not find evidence of it in our research.

If Commonwealth governments would like to contribute additional information to this report about activities in their respective countries, they are encouraged to reach out to the Cybersecurity Tech Accord at info@cybertechaccord.org.

For each country listed in the appendix, the following information is provided, as available:

GCI commitment: The cumulative rating provided by the GCI report on a nation's overall commitment to cybersecurity, with a rating of "Low," "Medium," or "High" based on legal, technical, organisational, capacity building, and cooperation indicators.²³

Awareness campaigns developed and implemented: Whether such campaigns either currently exist or have taken place in recent years.

Campaign targets: If there are awareness programs, this highlights whom they are intended for (Organisations/Civil society/Adults/Youth/Other groups).

National cyber agency: Whether or not a country has a dedicated agency for cybersecurity.

National Cybersecurity Awareness Month: Whether a country observes October, or any other month, as Cybersecurity Awareness Month.

Primary/secondary education programs: Whether the country reports having primary or secondary education programs focused on cybersecurity awareness.

National awareness program link(s): Links to further information on awareness programs and the agencies that sponsor them.

²¹ TU. *Global Cybersecurity Index (GCI)*, 2018. ITU Publications. Geneva, Switzerland. 2019. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf











²² NCSI: National Cyber Security Index. e-Governance Academy Foundation. Tallinn, Estonia. <https://ncsi.ega.ee/>




























²³ GCI, 2018

COMMONWEALTH NATIONS IN AFRICA



Country	Cybersecurity Capacity and Awareness Initiatives	
Botswana	GCI commitment:	Medium ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	N/A ○
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	N/A ○
	National awareness program link(s):	N/A ○
Cameroon	GCI commitment:	Medium ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	No ○
	National awareness program link(s):	https://www.antic.cm/
Gambia	GCI commitment:	Low ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	Yes ○
	Primary/secondary education programs:	N/A ○
	National awareness program link(s):	http://gamcybersecurityalliance.com/ https://mcjsupport.org/2019/01/29/data-privacy-day-19-the-gambia/ https://www.saferinternetday.org/web/gambia/sid
Ghana	GCI commitment:	Medium ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, adults, youth
	National cyber agency:	N/A ○
	National Cybersecurity Awareness Month:	Yes ○
	Primary/secondary education programs:	Yes ○
	National awareness program link(s):	https://cybersecurity.gov.gh/index.php/a-safer-digital-ghana-programme/

Kenya	GCI commitment:	High 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes 
	National Cybersecurity Awareness Month:	Yes 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://www.ke-cirt.go.ke/index.php/bulletins-and-guides/ http://www.userawarenessafrica.co.ke/
Lesotho	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	N/A 
	Campaign targets:	N/A 
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	N/A 
Malawi	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	N/A 
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	N/A 
Mauritius	GCI commitment:	High 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	Yes 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	Yes 
	National awareness program link(s):	http://cybersecurity.ncb.mu/English/Knowledge_bank/Pages/Guidelines.aspx
Mozambique	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://mozcyber.inage.gov.mz/




















Namibia	GCI commitment:	Low	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Youth	
	National cyber agency:	N/A	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	https://nncsc.com/	
Nigeria	GCI commitment:	Medium	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Organisations, civil society, adults, youth	
	National cyber agency:	Yes	
	National Cybersecurity Awareness Month:	Yes	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	https://certt.ng/Home/Services	
Rwanda	GCI commitment:	High	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Organisations, civil society, adults, youth, other groups	
	National cyber agency:	Yes	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	https://rwandacybersec.org/?page_id=77	
Seychelles	GCI commitment:	Low	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Organisations, adults, youth	
	National cyber agency:	N/A	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	https://www.police.gov.sc/about-us/be-alert	
Sierra Leone	GCI commitment:	Low	
	Awareness campaigns developed/implemented:	N/A	
	Campaign targets:	N/A	
	National Cybersecurity Awareness Month:	N/A	
	National cyber agency:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	N/A	

South Africa	GCI commitment:	Medium	○
	Awareness campaigns developed/implemented:	Yes	●
	Campaign targets:	Organisations, adults, youth	
	National cyber agency:	Yes	●
	National Cybersecurity Awareness Month:	Yes	●
	Primary/secondary education programs:	N/A	○
	National awareness program link(s):	https://www.cybersecurityhub.gov.za/cyberawareness/index.php/awareness-resources.html http://eagle.unisa.ac.za/elmarie/ http://www.cyberaware.org.za/	
Swaziland/ Eswatini	GCI commitment:	Low	○
	Awareness campaigns developed/implemented:	Yes	●
	Campaign targets:	Organisations, civil society, adults, youth	
	National cyber agency:	N/A	○
	National Cybersecurity Awareness Month:	Yes (Nov)	●
	Primary/secondary education programs:	N/A	○
	National awareness program link(s):	https://www.esccom.org.sz/cybersecurity/	
Uganda	GCI commitment:	Medium	○
	Awareness campaigns developed/implemented:	Yes	●
	Campaign targets:	Organisations, adults, youth, other groups	
	National cyber agency:	Yes	●
	National Cybersecurity Awareness Month:	N/A	○
	Primary/secondary education programs:	Yes	●
	National awareness program link(s):	https://www.nita.go.ug/publication/online-e-safety-educational-toolkit-young-people-uganda	
United Republic of Tanzania	GCI commitment:	Medium	○
	Awareness campaigns developed/implemented:	Yes	●
	Campaign targets:	Organisations, adults, youth	
	National cyber agency:	Yes	●
	National Cybersecurity Awareness Month:	N/A	○
	Primary/secondary education programs:	N/A	○
	National awareness program link(s):	N/A	

COMMONWEALTH NATIONS IN ASIA



Country	Cybersecurity Capacity and Awareness Initiatives	
Zambia	GCI commitment:	Medium ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	Yes ○
	National awareness program link(s):	www.zicta.zm Ehenet am faccusaped que la quo tem nos
Bangladesh	GCI commitment:	Medium ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	Yes ○
	Primary/secondary education programs:	N/A ○
	National awareness program link(s):	https://www.cirt.gov.bd/declaration-2017-on-strengthening-cybersecurity/
Brunei	GCI commitment:	Medium ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	N/A ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	Yes ○
	National awareness program link(s):	https://www.rbts.com.bn/iet-visit-to-rbts-training-simulation-centre-tsc-2/
India	GCI commitment:	High ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	Yes ○
	National awareness program link(s):	http://www.isea.gov.in/isea/home/index.html

Malaysia	GCI commitment:	High	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Organisations, civil society, adults, youth, other groups	
	National cyber agency:	Yes	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	Yes	
	National awareness program link(s):	https://www.cybersafe.my/en/	
Pakistan	GCI commitment:	Medium	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Youth	
	National cyber agency:	Yes	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	No	
	National awareness program link(s):	http://www.nccs.pk/nccs/what-we-do http://www.nccs.pk/activities/conference/conference-home	
Singapore	GCI commitment:	High	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Organisations, civil society, adults, youth, other groups	
	National cyber agency:	Yes	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	Yes	
	National awareness program link(s):	https://www.csa.gov.sg/gosafeonline https://www.imda.gov.sg/-/media/imda/files/inner/archive/news-and-events/news_and_events_level2/20070402172309/factsheet_csaa.pdf	
Sri Lanka	GCI commitment:	Medium	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Organisations, civil society, adults, youth, other groups	
	National cyber agency:	Yes	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	http://www.slcert.gov.lk/events.php	

COMMONWEALTH NATIONS IN THE CARIBBEAN & SOUTH AMERICA



Country	Cybersecurity Capacity and Awareness Initiatives	
Antigua and Barbuda	GCI commitment:	Low ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	N/A ○
	National awareness program link(s):	https://www.getsafeonline.ag/ https://www.antiguaobserver.com/information-ministry-hosts-cyber-workshop/
Bahamas	GCI commitment:	Low ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	N/A ○
	National awareness program link(s):	https://www.getsafeonline.bs/
Barbados	GCI commitment:	Low ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	https://www.getsafeonline.bb/ ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	N/A ○
	National awareness program link(s):	https://www.getsafeonline.bs/
Belize	GCI commitment:	Low ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	N/A ○
	National awareness program link(s):	https://cybersecurity.nigf.bz/ https://www.getsafeonline.bz/

Dominica	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://www.getsafeonline.dm/
Grenada	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://www.getsafeonline.gd/
Guyana	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	Yes 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://www.getsafeonline.gy https://cirt.gy/Tips
Jamaica	GCI commitment:	Medium 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	Yes 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://jis.gov.jm/october-is-cybersecurity-awareness-month/ https://www.getsafeonline.org.jm/

St Kitts and Nevis	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://www.getsafeonline.kn/
St Lucia	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://www.getsafeonline.lc/ https://stluciatimes.com/saint-lucia-hosts-caribbean-commonwealth-cyber-security-workshop/#comments
St Vincent and the Grenadines	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://www.getsafeonline.vc
Trinidad and Tobago	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	https://www.getsafeonline.tt/

COMMONWEALTH NATIONS IN EUROPE & NORTH AMERICA



Country	Cybersecurity Capacity and Awareness Initiatives
Malta	<p>GCI commitment: Medium ○</p> <p>Awareness campaigns developed/implemented: Yes ○</p> <p>Campaign targets: Organisations, civil society, adults, youth</p> <p>National cyber agency: Yes ○</p> <p>National Cybersecurity Awareness Month: Yes ○</p> <p>Primary/secondary education programs: Yes ○</p> <p>National awareness program link(s): https://mita.gov.mt/en/ict-features/Pages/2018/Launch-of-a-National-Cyber-Security-awareness-and-educational-campaign.aspx https://cybersecurity.gov.mt/past-events/</p>
Republic of Cyprus	<p>GCI commitment: Medium ○</p> <p>Awareness campaigns developed/implemented: Yes ○</p> <p>Campaign targets: Youth, other groups</p> <p>National cyber agency: Yes ○</p> <p>National Cybersecurity Awareness Month: Yes ○</p> <p>Primary/secondary education programs: Yes ○</p> <p>National awareness program link(s): https://ccsc.org.cy/call-for-the-2nd-cyprus-cyber-security-challenge-2019/</p>
United Kingdom	<p>GCI commitment: High ○</p> <p>Awareness campaigns developed/implemented: Yes ○</p> <p>Campaign targets: Organisations, civil society, adults, youth</p> <p>National cyber agency: Yes ○</p> <p>National Cybersecurity Awareness Month: Yes ○</p> <p>Primary/secondary education programs: Yes ○</p> <p>National awareness program link(s): https://www.cpni.gov.uk/security-awareness-campaigns https://www.ncsc.gov.uk/section/information-for/individuals-families https://cybersecuritymonth.eu/ecsm-countries/united-kingdom https://www.getsafeonline.org/ https://www.gov.uk/government/publications/essential-digital-skills-framework</p>



Canada	GCI commitment:	High ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	Yes ○
	Primary/secondary education programs:	Yes ○
	National awareness program link(s):	https://www.getcybersafe.gc.ca/cnt/rsrscs/csam-tlkt-en.aspx https://www.getprepared.gc.ca/cnt/rsrscs/sfttps/tp201010-en.aspx

COMMONWEALTH NATIONS IN OCEANIA





























Country Cybersecurity Capacity and Awareness Initiatives

Australia	GCI commitment:	High ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, children, other groups
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	Yes ○
	Primary/secondary education programs:	Yes ○
	National awareness program link(s):	https://www.cyber.gov.au/tags/stay-smart-online-sso https://www.cyber.gov.au/advice https://www.staysmartonline.gov.au/get-involved/stay-smart-online-week https://www.cyberchallenge.com.au/#thechallenge https://business.nt.gov.au/news/2018/cyber-security-awareness-month https://www.austcyber.com/node/44 https://aca.edu.au/projects/cyber-challenges/ https://aca.edu.au/projects/cyber-challenges/

Fiji	GCI commitment:	Low ○
	Awareness campaigns developed/implemented:	Yes ○
	Campaign targets:	Organisations, civil society, adults, children, other groups
	National cyber agency:	Yes ○
	National Cybersecurity Awareness Month:	N/A ○
	Primary/secondary education programs:	N/A ○
National awareness program link(s):	https://www.saferinternetday.org/web/fiji/sid	

Kiribati	GCI commitment:	Low	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Adults, youth	
	National cyber agency:	Yes	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	https://www.cybersafetypasifika.org/	
Nauru	GCI commitment:	Low	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Youth	
	National cyber agency:	N/A	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	N/A	
New Zealand	GCI commitment:	High	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Organisations, civil society, adults, youth	
	National cyber agency:	Yes	
	National Cybersecurity Awareness Month:	Yes	
	Primary/secondary education programs:	Yes	
	National awareness program link(s):	https://www.netsafe.org.nz/safer-internet-day/ https://www.ncsc.govt.nz/about-us/	
Papua New Guinea	GCI commitment:	Low	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	Youth	
	National cyber agency:	N/A	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	https://www.nicta.gov.pg/2019/02/safer-internet-day-2019/	
Samoa	GCI commitment:	Medium	
	Awareness campaigns developed/implemented:	Yes	
	Campaign targets:	N/A	
	National cyber agency:	N/A	
	National Cybersecurity Awareness Month:	N/A	
	Primary/secondary education programs:	N/A	
	National awareness program link(s):	N/A	

Solomon Islands	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	N/A 
	Campaign targets:	N/A 
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	N/A 
Tonga	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	Yes 
	Campaign targets:	Organisations, adults, youth
	National cyber agency:	Yes 
	National Cybersecurity Awareness Month:	Yes 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	http://www.gov.to/press-release/tonga-marks-cyber-security-awareness-month/ http://www.mic.gov.to/news-today/press-releases/5576-tonga-moving-forward-in-promoting-cyber-safety--national-cyber-safety-week http://www.gov.to/press-release/tonga-cert-conducts-trainings-to-the-island-group-of-haapai/ www.stopthinkconnect.gov.to
Tuvalu	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	N/A 
	Campaign targets:	N/A 
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	N/A 
Vanuatu	GCI commitment:	Low 
	Awareness campaigns developed/implemented:	N/A 
	Campaign targets:	N/A 
	National cyber agency:	N/A 
	National Cybersecurity Awareness Month:	N/A 
	Primary/secondary education programs:	N/A 
	National awareness program link(s):	N/A 



WWW.CYBERTECHACCORD.ORG