2019

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

DRAFT DOCUMENT 1.1

Foreign & Commonwealth Office

The Commonwealth

EXECUTIVE SUMMARY

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"). The organisation spans across the entire globe and includes nations of all levels of economic development, as well as a wide range of cultures and populations. This wealth of diversity results in very different approaches to cybersecurity awareness, and very different needs when it comes to building a culture of cybersecurity. This report highlights many of the different ways Commonwealth nations are promoting greater cybersecurity awareness and is being released in October to draw more attention to this important issue during the 2019 Cybersecurity Awareness Month.

This report 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. While not intended to evaluate any particular cybersecurity awareness program, the report provides 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.

Finally, the report explores the different ways in which countries across the Commonwealth are choosing the promote cybersecurity awareness in their local contexts, highlighting what types of activities are 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 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 within their own countries based on the learnings and efforts of others in the Commonwealth.

INDEX

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 for the first time each year and joining the greatest experiment in human history – the public 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, knowing 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. Thankfully, these types of attacks can be easily defending against by practicing basic cyber hygiene and maintaining awareness of the threats that exist online. However, such cybersecurity awareness needs to be intentionally built through public awareness and education initiatives, and ideally with the support of the technology industry.

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 cyber 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 100 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.

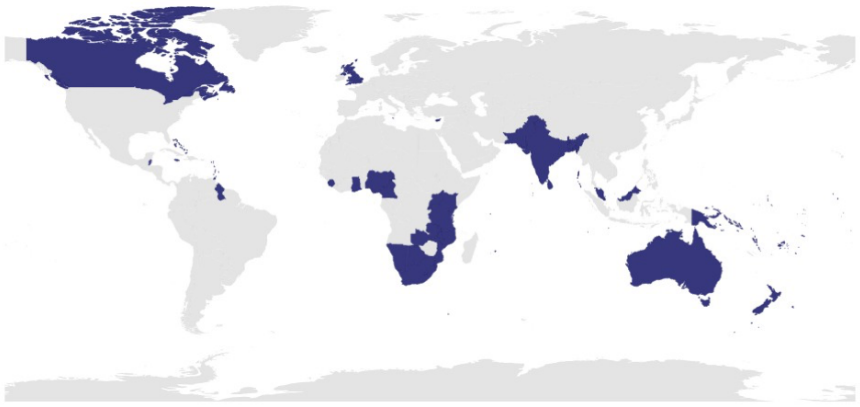
These capacity building efforts are aligned with the third principle of the Accord – *We will help empower users, customers and developers to strengthen cybersecurity protection* – and underscores the responsibility the technology industry has for supporting users and customers in understanding how to use technology products and services safely and to minimize 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 generalizations. 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 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

Given its commitment to cross-cultural learning, capacity building, and development, the Cybersecurity Tech Accord is incredibly proud to join with the Commonwealth in helping facilitate an exchange between member states on a topic that is perfectly aligned with its own commitments – *cybersecurity awareness*. Over several months between 2018 and 2019, the signatories of the Cybersecurity Tech Accord have been working in coordination with the United Kingdom's Foreign & Commonwealth Office to conduct a preliminary study of the different approaches to cybersecurity awareness across the Commonwealth.

This study has included a 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. This summative report presents the findings from this initial 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, underscoring the importance of a multistakeholder approach;

III. Provide recommendations on cybersecurity awareness initiatives that have proved effective from the perspective of the technology industry; and,

IV. 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. Tallin, 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" to begin with, which is often understood differently in different contexts. Leveraging one helpful and comprehensive definition provided by Cisco Systems:

> ***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 to and how to mitigate them.

Cybersecurity is a relatively new challenge, one that has only truly developed over the past generation with the advent of the modern public Internet and all the devices it connects today. Despite its limited history, cybersecurity increasingly impacts every individual, organisation and government on the planet that relies on the use of computer networks. However, while

[5] Cisco Systems. What is Cybersecuirty? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

cybersecurity 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.

[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 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 "*cyber 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 important policies and regulations that governments can pursue in this effort as well, nothing can replace the impact of a healthy culture of cybersecurity awareness. Such a culture can and should 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. These programs can take many different forms, including setting aside particular time to recognise the importance of cybersecurity, like during 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 EXAMPLES[11]

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 audience 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."

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."

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 and beyond 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 off 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 cybersecurity awareness programs, we recommend exploring the good practices and guidance materials made available by the GFCE, including the Cybersecurity Awareness Toolkit developed by the Organisation of American States, which are available here: https://www.thegfce.com/good-practices/cyber-security-awareness.

SNAPSHOT: CYBERSECURITY AWARENESS ACROSS THE COMMONWEALTH OF NATIONS

As mentioned previously, the Commonwealth is an incredibly diverse coalition of 53 countries spread across the world. This diversity is especially pronounced when it comes to relative measures of cybersecurity capacity and awareness between member states. This section provides a high-level overview of this dynamic across the entire Commonwealth 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.

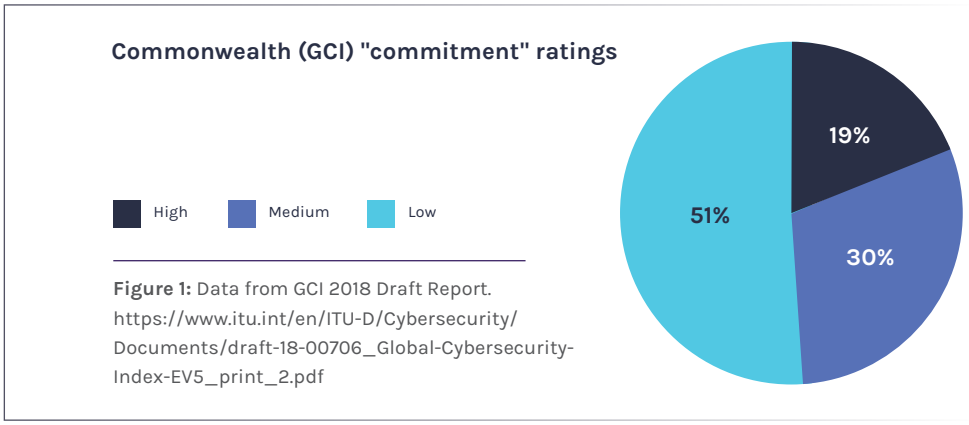


Figure 1: Data from GCI 2018 Draft Report. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

As can be seen, 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 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 the 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 an ideal association 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.

Drilling down into this dataset further, the GCI data provides 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.[13]

There is also a wide diversity in the types of awareness programs that countries focus on throughout the Commonwealth – targeting different age groups and sectors – as reflected in the chart below. While only one targeted sub-population (youth & children) has awareness programs targeting them in more than 50% of the Commonwealth, civil society in particular lags behind in terms of public awareness programs targeting them.

Cyber awareness program targets in Commonwealth (GCI)

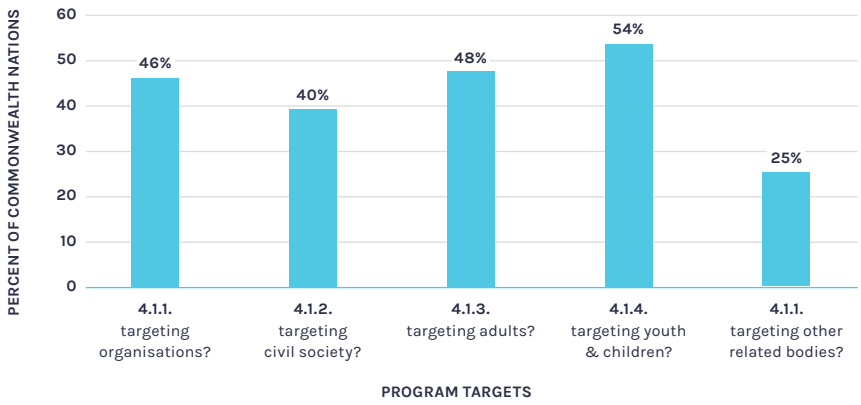


Figure 2: Data shared by ITU from 2018 Survey

One leading way in which many countries around 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 an international campaign led by US, Canadian, and EU diplomatic efforts. However, despite the international encouragement, 39 of the 53 Commonwealth countries do not yet appear to recognise October, or any month, as Cybersecurity Awareness Month based on internal research. While the entirety of the EU has embraced October as the month for this observance, large pockets of Africa and the Caribbean in particular appear to have not yet dedicated a month to promote cybersecurity.

[13] Ibid

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." A simple but effective concept, Cybersecurity Awareness Month is an annual public campaign, recognised now in dozens of countries, setting aside the month of October to focus on educating citizens about how to stay safe online. While it is just one example of a public campaign focused on this issue, there are several reasons why the recognition of Cybersecurity Awareness Month provides an effective structure for promoting meaningful awareness in keeping with the principles outlined above.

The benefits of embracing National Cybersecurity Awareness Month (NCAM) in October begin with its structure as a regular annual event. As mentioned earlier, cybersecurity is not a box to be checked and set aside, it is something that needs to be continually practiced and performed. Similarly, cybersecurity awareness initiatives need to be ongoing and recursive. Setting aside October each year as time for the public to re-engage with this topic is a meaningful way to build and maintain a culture of cybersecurity awareness.

Having a regular, annual campaign also allows the messaging on cybersecurity awareness to remain current. Cyber threats evolve and change, and so too must our awareness and understanding of good cybersecurity practices to stay up to date. The challenges of today will not be the same as tomorrow, but we know they will exist and that we will have to re-educate ourselves. Governments that recognise NCAM embrace this dynamic by using each October as a time to spotlight the different, and frequently new, cyber threats and what citizens can do to remain safe online. Some recent examples include:

- **United States** – The 2018 themes for NCAM in the US were broken down by week, and included "strengthen the cybersecurity workforce," and "secure critical infrastructure from cybersecurity threats."[14]
- **European Union** – The European Union has supported the adoption of October as Cybersecurity Awareness Month across all its member states, with activities coordinated by the European cybersecurity agency (ENISA). The 2018 themes for the EU's cybersecurity month included "recognizing cyber scams" and "emerging technologies and privacy."[15]

[14] National Cybersecurity Awareness Month. Department of Homeland Security. 2019 https://www.dhs.gov/national-cyber-security-awareness-month

[15] European Cyber Security Month 2018. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/events/european-cyber-security-month-2018

- **Canada** – Canada maintains an online dashboard with shareable resources aligned to the themes of NCAM each year. This year's themes address 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."[16]
- **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.[17]

Indeed, having 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. However, while all nations may recognise the same cybersecurity awareness month, their respective efforts during that time will differ. As the above examples also suggest, another benefit of recognising NCAM is that it allows for a global initiative to be differentiated by local context.

There are tremendous benefits in governments recognising and embracing October as NCAM to motivate further action and as a rallying cry for citizens to take notice of an important issue. In fact, it is no coincidence that the first release of this paper is happening alongside Cybersecurity Awareness Month in October of 2019. Especially for countries that have not pursued other cybersecurity awareness initiatives previously, 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. 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.

[16] *Cyber Security Awareness Month Toolkit. Government of Canada.* https://www.getcybersafe.gc.ca/cnt/rsrcs/csam-tlkt-en.aspx

[17] Cybersecurity Awareness Month. Northern Territory Government. September 2018. https://business.nt.gov.au/news/2018/cyber-security-awareness-month

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,

IV. hackathons/competitions,

V. cybersecurity awareness organisations, and

VI. cybersecurity awareness education.

Each of these approaches provides a unique way to increase cybersecurity awareness and, similar to public health campaigns, generally the more ways good information can be shared to increase public awareness of cyber risk and best practices, the better. Cybersecurity Awareness Month, as one example, would certainly fit within "national awareness campaigns," though we have chosen dedicate the previous section to it as a particularly valuable and timely global campaign.

The examples provided below are not intended to be exhaustive of all such efforts taking place in the Commonwealth, but should provide a good sense of what initiatives are being pursued by this collection of countries, and what they can look like in practice. In addition, it should be noted that while we group the initiatives based on common characteristics, many nations are pursuing multiple 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 in October, as a way of bringing more attention to the issue at an optimal time.

As stated earlier, the intent of this report is not to judge or evaluate respective awareness programs or initiatives, all of which may have value in promoting greater public awareness and security. However, any approaches to promoting cybersecurity awareness, including the examples highlighted in this section, should be considered in light of the framework previously provided – how well do they facilitate national cybersecurity awareness in a way that is "up-to-date," "recursive," "inclusive," "culturally responsive" and "multistakeholder" in nature? While few programs may check all of these boxes in a meaningful way, this helpful framework can provide a good reference point for understanding how comprehensive any particular initiative is likely to be and what could be effective ways to improve them.

NATIONAL CYBER AWARENESS CAMPAIGNS

Several nations in the Commonwealth have implemented ongoing national campaigns intended to promote and reinforce cybersecurity awareness. Similar to Cybersecurity Awareness Month, these types of campaigns are helpful in directing national attention towards a pressing topic for a period of time. These campaigns are uniquely well suited to highlighting discrete cyber threats or habits that citizens need to be aware of in a timely fashion, as well as for targeting specific demographics within a country that may need particular support. These campaigns can include public awareness announcements – such as targeted advertisements, and public remarks made by elected officials – and may also include more on-the-ground work to bring messaging to specific communities through locally-hosted events and activities.

Commonwealth example(s):

1

National Cyber Security awareness and educational campaign – Malta

In Malta, the nation is in the midst of a 2-year cybersecurity awareness campaign first launched in 2018. According to officials, the campaign is intended to keep the public better informed about risks as more and more consumer and social behavior moves online. The campaign is deliberately intended to reach across social strata in the country to make sure the entire public is made aware of best practices for staying safe online. The campaign began with a public survey to establish a baseline understanding of cybersecurity awareness and where critical gaps may exist. The campaign was launched alongside the recognition of 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

2

Security Awareness Campaigns – United Kingdom

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 CYBER AWARENESS WORKSHOPS

Cyber awareness workshops are becoming increasingly common events where governments try to bring together key stakeholders 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 current gaps in cybersecurity awareness and how they can be addressed. They can also be focused on reaching out to and including stakeholder groups or particular populations that are most in need of improved cybersecurity awareness.

The impact and effectiveness of such a workshop is likely to be dependent as much on who attends as by what particular content is communicated. These workshops may target 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 leaders from these organisations in attendance in order to take back and communicate the workshop's messaging following the event. Failure to have the right people in the room can result in a well-developed workshop with blunted impact when the resources and knowledge provided are not communicated further.

Commonwealth example(s):

1

Get Safe Online Awareness Workshops – Caribbean

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 Commonwealth nations in the region.

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

2

National Cyber Security Symposium – Belize

This week-long workshop in Belize is hosted by several governmental offices – including the Ministry of Home Affairs, Attorney General, and the Belize National Internet Governance forum – with sponsorship support from corporate partners as well. The workshop focuses on promoting awareness of the current cyber threats faced in Belize among essential stakeholders. The week kicks off by recognizing a "National Cybersecurity Awareness Day," with later days of the event differentiating content for different government sectors, including law enforcement, as well as sessions for the business community.

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

3

Cyber Security Forum – Brunei

This gathering is hosted by the Royal Brunei Technical Services, with sponsorship as well from a domestic private sector partner. The gathering focused on facilitating greater awareness among corporations operating in the country about contemporary cyber threats and ways organisations can operate safely online. The forum features prominent speakers from the nation's security ministry, as well as representatives from public and private sector focused on telecommunications, ICT and energy.

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

CYBERSECURITY AWARENESS DIGITAL RESOURCES

National campaigns and initiatives, like those outlined above, can only do so much to share critical messaging on cybersecurity awareness with citizens. As a result, many countries are increasingly hosting content on cybersecurity awareness on government websites. While the Internet is awash with resources highlighting cybersecurity best practices – many of which are just an Internet search away – 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. 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. In addition to the examples from the Commonwealth provided below, the Cybersecurity Tech Accord maintains an ever-growing webinar series on a range of current cybersecurity topics on its website, which it develops in partnership with the Global Forum for Cyber Expertise (GFCE), serving as a valuable free resource that is available here: https://cybertechaccord.org/webinars/

Commonwealth example(s):

1

Get Safe Online – United Kingdom & the Caribbean

Sponsored by the 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 – with specific subsections on protecting devices, personal information and children online, as well as how to responsibly use online services like banking and social networks. In addition to its resource hub, Get Safe Online also has regionally specific versions of its content in the form of customized websites for Commonwealth nations in the Caribbean.

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

Commonwealth content: https://www.getsafeonline.org/commonwealth/

2

General Information Security Guidelines – Mauritius

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

3

NCSC's Information for... – United Kingdom

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/

4

CyberSafe TT – Trinidad and Tobago

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/

5

Cyber Tips & Advice – South Africa

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

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

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 into the discussion. These competitions can be structured to focus on a particular topic, or simply invite proposals for addressing cybersecurity challenges 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 uniquely focused on promoting cybersecurity awareness, these hackathons can result in greater awareness and engagement among non-traditional populations on cybersecurity challenges.

Commonwealth example(s):

1

CyberFirst Girls Competition – United Kingdom

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 customized cybersecurity challenges designed to align with the UK's computer science curricula while introducing more advanced topics in cybersecurity as well. While the

competition is supposed to push student thinking, 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

2

Cyprus Cyber Security Challenge – Cyprus

Sponsored by a combination of private and public entities, and coordinated by a nonprofit, the Cyprus Cyber Security Challenge is an annual event targeting youth populations that encourages participation by hackers and security professionals, as well as those from nontraditional backgrounds, to try and solve cybersecurity challenges. The goal is to try and identify talented individuals who may not have previously considered a career in cybersecurity, by having participants compete in teams to solve a number of problems related to web security, mobile security, crypto puzzles, reverse engineering and forensics. Winners are able to compete in the European Cyber Security Challenge during Cybersecurity Awareness Month in October.

More information: https://ccsc.org.cy/call-for-the-2nd-cyprus-cyber-security-challenge-2019/

3

Cyber Security Challenge Australia – Australia

The Cyber Security Challenge Australia (CyCSA) is an annual program in October 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/

CYBERSECURITY AWARENESS ORGANISATIONS

Nearly all of 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. This is why many nations have established organisations dedicated to coordinating cybersecurity awareness as an essential part of their mandate. These organisations can be differently structured – some are part of dedicated cybersecurity agencies operated by governments, others are housed as part of other departments, while still others exist as organisations that operate independent of a particular government.

Developing a public 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 can coordinate a multifaceted approach to building cybersecurity awareness, evaluate the progress of respective programs, and identify gaps within public awareness that should be further addressed.

Commonwealth example(s):

1

Get Cyber Safe – Canada

This program is operated within the Canadian Centre for Cyber Security and serves as the primary public interface for the organisation, which 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

Gambia Cyber Security Alliance – The Gambia

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

More information: http://gamcybersecurityalliance.com/

3

Cyber Security Awareness Alliance – Singapore

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

4

National Cyber Security Centre – Ghana

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, general public, government agencies, and businesses.

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

5

National Data Management Authority, Computer Incident Response Team – Guyana

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/

6

NetSafe – New Zealand

NetSafe is an independent nonprofit 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/

7

National Agency for Information and Communication Technologies – Rwanda

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

8

CyberSAFE – Malaysia

The 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/

CYBERSECURITY AWARENESS EDUCATION

Getting students familiar with cyber risk and cyber hygiene from an early age, and continuing to reinforce good practices as they move through school, is an essential way in which government policy can help build an enduring culture of cybersecurity. As students are expected to increasingly use technology as part of their education, the requisite training on how to stay safe in doing so should be a core component of any curriculum. While further guidance on how to develop and implement an effective cybersecurity curriculum go beyond the scope of this report – and indeed could easily fill a separate and worthwhile study – the importance of such programs for building a culture of cybersecurity warranted recognition here.

APPENDIX — COMMONWEALTH COUNTRY OVERVIEWS

The following section provides an overview of the cybersecurity capacities and resources that exist within each respective Commonwealth country 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,[18] [19] 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. As stated earlier, 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.[20]

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.

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.

---

[18] 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

[19] NCSI: National Cyber Security Index. e-Governance Academy Foundation. Tallin, Estonia. https://ncsi.ega.ee/

[20] 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
	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
	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
	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/*
Ghana	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, adults, youth
	National cyber agency:	N/A
	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:	N/A
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A
Lesotho	GCI commitment:	Low
	Awareness campaigns developed/implemented:	N/A
	Campaign targets:	N/A
	National cyber agency:	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
	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
	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:	N/A
	Campaign targets:	N/A
	National cyber agency:	N/A
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A

Namibia	GCI commitment:	Low
	Awareness campaigns developed/implemented:	N/A
	Campaign targets:	N/A
	National cyber agency:	N/A
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A
Nigeria	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes
	Primary/secondary education programs:	N/A
	National awareness program link(s):	*https://cerrt.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
	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
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A
Sierra Leone	GCI commitment:	Low
	Awareness campaigns developed/implemented:	N/A
	Campaign targets:	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
	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/	
Swaziland/ Eswatini	GCI commitment:	Low
	Awareness campaigns developed/implemented:	N/A
	Campaign targets:	N/A
	National cyber agency:	N/A
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A
Uganda	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, adults, youth, other groups
	National cyber agency:	N/A
	Primary/secondary education programs:	Yes
	National awareness program link(s):	N/A
United Republic of Tanzania	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, adults, youth
	National cyber agency:	Yes
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A
Zambia	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	Yes
	Primary/secondary education programs:	Yes
	National awareness program link(s):	
	www.zicta.zm	

COMMONWEALTH NATIONS IN ASIA

Country	Cybersecurity Capacity and Awareness Initiatives	
Bangladesh	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes
	Primary/secondary education programs:	N/A
	National awareness program link(s):	
	https://www.cirt.gov.bd/declaration-2017-on-strengthening-cybersecurity/	
India	GCI commitment:	High
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	Yes
	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
	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
	Primary/secondary education programs:	No
	National awareness program link(s):	N/A

Singapore	GCI commitment:	High
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth, other groups
	National cyber agency:	Yes
	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
	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:	Civil society, adults, youth
	National cyber agency:	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:	N/A
	Campaign targets:	N/A
	National cyber agency:	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:	N/A
	Campaign targets:	N/A
	National cyber agency: https://www.getsafeonline.bb/	
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A
Belize	GCI commitment:	Low
	Awareness campaigns developed/implemented:	N/A
	Campaign targets:	N/A
	National cyber agency:	Yes
	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:	N/A
	Campaign targets:	N/A
	National cyber agency:	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:	N/A
	Campaign targets:	N/A
	National cyber agency:	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:	N/A
	Campaign targets:	N/A
	National cyber agency:	N/A
	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
	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:	N/A
	Campaign targets:	N/A
	National cyber agency:	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:	N/A
	Campaign targets:	N/A
	National cyber agency:	N/A
	Primary/secondary education programs:	N/A
	National awareness program link(s):	
	https://www.getsafeonline.lc/	

St Vincent and the Grenadines	GCI commitment:	Low
	Awareness campaigns developed/implemented:	N/A
	Campaign targets:	N/A
	National cyber agency:	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:	N/A
	Campaign targets:	N/A
	National cyber agency:	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	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes
	Primary/secondary education programs:	Yes
	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/	
Republic of Cyprus	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets: Youth, other groups	
	National cyber agency:	Yes
	Primary/secondary education programs:	Yes
	National awareness program link(s):	
	https://ccsc.org.cy/call-for-the-2nd-cyprus-cyber-security-challenge-2019/	

United Kingdom	GCI commitment:	High
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes
	Primary/secondary education programs:	Yes
	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/	
Brunei	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	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/	

Canada	GCI commitment:	High
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, youth
	National cyber agency:	Yes
	Primary/secondary education programs:	Yes
	National awareness program link(s):	
	https://www.getcybersafe.gc.ca/cnt/rsrcs/csam-tlkt-en.aspx	
	https://www.getprepared.gc.ca/cnt/rsrcs/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
	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	
Fiji	GCI commitment:	Low
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Organisations, civil society, adults, children, other groups
	National cyber agency:	Yes
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A
Kiribati	GCI commitment:	Low
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	Adults, youth
	National cyber agency:	Yes
	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
	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
	Primary/secondary education programs:	Yes
	National awareness program link(s):	*https://www.netsafe.org.nz/safer-internet-day/*
Papua New Guinea	GCI commitment:	Low
	Awareness campaigns developed/implemented:	N/A
	Campaign targets:	N/A
	National cyber agency:	N/A
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A
Samoa	GCI commitment:	Medium
	Awareness campaigns developed/implemented:	Yes
	Campaign targets:	N/A
	National cyber agency:	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
	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
	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
	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
	Primary/secondary education programs:	N/A
	National awareness program link(s):	N/A

WWW.CYBERTECHACCORD.ORG